Rec'd PCT/PTO 28 FEB 2002

ATTORNEY'S DOCKET NO: 020234

U.S. DEPARTMENT OF COMMERCE, PATENT AND TRADEMARK OFFICE		DATE: **February 28, 2002**
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		U.S. APPLN. NO. (if known): **10/069118**
INTERNATIONAL APPLICATION NO.: **PCT/JP00/05832**	INTERNATIONAL FILING DATE: **AUGUST 29, 2000**	PRIORITY DATE CLAIMED: **AUGUST 30, 1999**

TITLE OF INVENTION: ***DATA REPRODUCTION APPARATUS***

APPLICANT(S) FOR DO/EO/US: **Masayuki HATANAKA, Jun KAMADA, Takahisa HATAKEYAMA, Takayuki HASEBE, Seigou KOTANI, Shigeki FURUTA, Takeaki ANAZAWA, Toshiaki HIOKI, Miwa KANAMORI and Yoshihiro HORI**

Applicant hereby submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. X This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.

2. ___ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.

3. X This express request to begin national examination procedures (35 USC 371(f)) at any time rather than delay examination until the expiration of the time limit set in 35 USC 371(b) and PCT Articles 22 and 39(1).

4. X A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. X A copy of the International Application as filed (35 U.S.C. 371(c)(2)):

   a. ___ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. X has been transmitted by the International Bureau.
   c. ___ is not required, as the application was filed in the United States Receiving Office (RO/US)

6. X A translation of the International Application into English (35 U.S.C. 371(c)(2)).

7. X Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))

   a. ___ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ___ have been transmitted by the International Bureau.
   c. ___ have not been made; however, the time limit for making such amendments has NOT expired.
   d. X have not been made and will not be made.

8. ___ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).

9. ___ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. X A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

ITEMS 11. TO 16. BELOW CONCERN OTHER DOCUMENT(S) OR INFORMATION INCLUDED:

11. **X** An Information Disclosure Statement under 37 CFR 1.97 and 1.98 together with the international search report and 8 Refs.

12. _ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
ASSIGNEE NAME AND ADDRESS: ***(1) FUJITSU LIMITED, Kanagawa, Japan; (2) NIPPON COLUMBIA CO., LTD., Tokyo, Japan; and (3) SANYO ELECTRIC CO., LTD., Moriguchi-shi, Japan***
Please publish the assignee data with the application.

13. X A **FIRST** preliminary amendment.

14. ___ A substitute specification.

15. ___ A change of power of attorney and/or address letter.

16. X Other items or information: 22 sheets of drawings.

U.S. APPLICATION NO. (if known) 10/069118	INTERNATIONAL APPLICATION NO. PCT/JP00/05832	DATE: February 28, 2002

17. X The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5): Search Report has been prepared by the EPO or JPO: $890.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) $710.00		
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) $740.00		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO $1040.00		
International preliminary examination fee (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) $100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	**$ 890.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than __ 20 X 30 months from the earliest claimed priority date (37 DVR 1.492(e)).	**$ 130.00**	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
TOTAL	41-20 =	21	X $ 18.00	**$ 378.00**	
INDEPENDENT	5 - 3 =	2	X $ 84.00	**$ 168.00**	
Multiple dependent claims(s) (if applicable)			+ $280.00		
			TOTAL OF ABOVE CALCULATIONS =	**$1,566.00**	
Reduction by 1/2 for filing by small entity, if applicable. (Note 37 CFR 1.9, 1.27, 1.28).					
			SUBTOTAL =	**$1,566.00**	
Processing fee of **$130.00** for furnishing the English translation later than __ 20 __ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +					
			TOTAL NATIONAL FEE =	**$1,566.00**	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00 per property +**					
			TOTAL FEES ENCLOSED =	**$1,566.00**	
				Amount to be: refunded	$
				charged	$

10069118.061102
JC19 Rec'd PCT/PTO 28 FEB 2002

ATTORNEY'S DOCKET NO: **020234**

U.S. APPLICATION NO. (if known) 10/069118	INTERNATIONAL APPLICATION NO. PCT/JP00/05832	DATE: **February 28, 2002**

a. X A check in the amount of $1,566.00 to cover the above fees is enclosed. ($890.00 for basic filing fee; $130.00 for late filing of the declaration, $378.00 for 21 additional claims, and $168.00 for 2 additional independent claims). (This paper is filed in triplicate)

b. ___ Please charge my Deposit Account No. 01-2340 in the amount of $___ to cover the above fees. (A duplicate copy of this sheet is enclosed.)

c. X The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 01-2340.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed to request that the application be restored to pending status.

Send All Correspondence To:

23850

PATENT TRADEMARK OFFICE

SIGNATURE

Mel R. Quintos

NAME

31,898

REGISTRATION NUMBER

MRQ/yap

ARMSTRONG, WESTERMAN & HATTORI, LLP
Suite 1000,1725 K Street, N W.
Washington, D. C 20006
Tel: (202) 659-2930
Fax: (202) 887-0357

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Masayuki HATANAKA et al.**

Serial No.: **Not Yet Assigned**
(§ 371 of International Application No. PCT/JP00/05832)

Filed: **February 28, 2002**

For: **DATA REPRODUCTION APPARATUS**

SUBMISSION OF SUBSTITUTE PAGES FOR PCT ART. 19 AND 34 AMENDMENTS AND PRELIMINARY AMENDMENT

Commissioner for Patents
Washington, D.C. 20231

February 28, 2002

Sir:

This application is the U.S. national stage under 35 USC § 371 of the above-identified international patent application. Please enter the attached substitute sheets for pages 1- 3, 3/1, 3/2, 3/3 and 3/4 of the specification. The substitute sheets incorporate into the English language translation of the international application amendments presented in the international stage under PCT Article 19 and /or PCT Article 34.

IN THE TITLE:

Please amend the title of the invention, in its entirety, so as to read as follows:

DATA REPRODUCTION APPARATUS AND DATA REPRODUCTION MODULE

IN THE CLAIMS:

Please cancel claims 1-22, without prejudice or disclaimer, and add claims 23-63 as follows:

23. A data reproduction apparatus (200) decrypting encrypted content data to reproduce content data, comprising:

a data reproduction unit (1500) to reproduce said encrypted content data, and

a data storage unit (120) storing said encrypted content data and an encrypted content key that is a content key directed to decrypt said encrypted content data in an encrypted form decryptable with a first decryption key unique to said data reproduction unit, and providing said encrypted content data and said encrypted content key to said data reproduction unit,

wherein said data reproduction unit comprises

a session key generation unit (1520) generating a session key updated at every access to obtain said content key with respect to said data storage unit,

a first encryption processing unit (1540) encrypting said session key using a public encryption key that can be decrypted at said data storage unit and that is unique to said data storage unit, and providing said encrypted session key to said data storage unit,

a first decryption processing unit (1506) using said session key to decrypt said encrypted content key obtained from said data storage unit in an encrypted form with said session key,

a first key hold unit (1540) prestoring said first decryption key,

a second decryption processing unit (1530) extracting said content key by applying a decryption process on an output from said first decryption processing unit using said first decryption key stored in said first key hold unit, and

a third decryption processing unit (1520) receiving said encrypted content data read out from said data storage unit to decrypt said encrypted content data using a content key extracted by said second decryption processing unit to extract content data.

24. The data reproduction apparatus according to claim 23, said content data being coded audio data coded according to a coding scheme to reduce an amount of data,

wherein said data reproduction unit comprises

an audio decoding unit (1508) reproducing audio data based on said coding scheme from said coded audio data, and

a digital-analog converter (1512) converting said reproduced audio data into an analog signal.

25. The data reproduction apparatus according to claim 23, wherein said data reproduction unit is provided in a security region that cannot be read out by a third party.

26. The data reproduction apparatus according to claim 23, wherein said data storage unit (120) comprises

a record unit (1412) to store data applied to said data storage unit,

a second key hold unit (1401) storing said public encryption key unique to said data storage unit, and that can supply said public encryption key to said data reproduction unit,

a third key hold unit (1402) storing a second decryption key used to decrypt data encrypted with said public encryption key,

a fourth decryption processing unit (1404) using said second decryption key to decrypt said first session key transmitted from said data reproduction unit in an encrypted form by said public encryption key, and

a second encryption processing unit (1406) encrypting encrypted content key stored in said recording unit using said first session key extracted at said fourth decryption processing unit for output.

27. The data reproduction apparatus according to claim 23, wherein said data storage unit is detachable with respect to said data reproduction unit.

28. A data reproduction apparatus (300, 400) decrypting encrypted content data to reproduce content data, comprising:

a data reproduction unit (1500) decrypting said encrypted content data using a content key directed to decrypt said encrypted content data to reproduce content data, and

a data storage unit (130, 140) storing said encrypted content data and said content key, and encrypting a first session key differing for every access to obtain said content key into a form

decryptable by a unique decryption key unique to said data reproduction unit for supply to said data reproduction unit,

wherein said data reproduction unit comprises

a first key hold unit (1540) prestoring said unique decryption key,

a first decryption processing unit (1530) applying a decryption processing using said unique decryption key which is an output from said first key hold unit,

a first session key generation unit (1522) generating a second session key updated for every access to obtain said content key with respect to said data storage unit,

a first encryption processing unit (1554) encrypting and applying to said data storage unit said second session key using a first session key that is encrypted in a form decryptable with said unique decryption key supplied from said data storage unit and decrypted at said first decryption processing unit, and

a second decryption processing unit (1556) decrypting for said second session key said content key supplied from said data storage unit in an encrypted form decryptable by said unique decryption key and further encrypted with said second session key,

said first decryption processing unit extracting said content key by applying a further decryption process on the output from said second decryption processing unit using said unique decryption key,

wherein said data reproduction unit further comprises a third decryption processing unit (1520) receiving said encrypted content data supplied from said data storage unit to decrypt said

receive encrypted content data using a content key extracted by said first decryption processing unit to extract content data.

29. The data reproduction apparatus according to claim 28, wherein said content data is coded audio data encoded by a coding scheme to reduce an amount of data,

wherein said data reproduction unit further comprises

an audio decoding unit reproducing audio data based on said coding method from said coded audio data, and

a digital-analog converter converting said reproduced audio data into an analog signal.

30. The data reproduction apparatus according to claim 29, wherein said data reproduction unit has at least said first key hold unit, said first decryption processing unit, said second decryption processing unit and said third decryption processing unit provided in a security region that cannot be read out by a third party.

31. The data reproduction apparatus according to claim 28, wherein said data storage unit (130, 140) comprises

a recording unit (1412) to store data applied to said data storage unit,

a second session key generation unit (1450) generating said first session key,

a second encryption processing unit (1452) applying an encryption process using a public encryption key unique to said data reproduction unit and directed to apply encryption that can be decrypted with said unique decryption key,

a fourth decryption processing unit (1454) using said first session key to decrypt said second session key transmitted from said data reproduction unit in an encrypted form with said first session key, and

a third encryption processing unit (1456) carrying out an encryption process by said first session key extracted at said fourth decryption processing unit for output,

said content key stored in said recording unit being encrypted at said second encryption processing unit and further encrypted at said third encryption processing unit to be supplied to said data reproduction unit.

32. The data reproduction apparatus according to claim 28, wherein said data storage unit is a memory card detachable with respect to said data reproduction unit.

33. The data reproduction apparatus according to claim 31, further comprising an authentication data hold unit (1560) storing and supplying to said data storage unit authentication data unique to said data reproduction unit together with said public encryption key in an encrypted form decryptable by an authentication key at said data storage unit,

wherein said data storage unit (140) comprises

a fifth decryption processing unit (1460) decrypting and extracting said authentication data and said public encryption key applied from said data reproduction unit in an encrypted form by said authentication key, and

control means carrying out an authentication process to determine whether to output said content key to a data reproduction unit from which said authentication data is output based on said authentication data extracted by said fifth decryption processing unit.

34. A data reproduction apparatus (500, 600) decrypting encrypted content data to reproduce content data, comprising:

a data reproduction unit decrypting said encrypted content data using a content key directed to decrypt said encrypted content data to reproduce content data, and

a data storage unit (150, 160) storing said encrypted content data and said content key, and encrypting and supplying to said data reproduction unit a first session key differing for every access to obtain said encrypted content data in an encrypted form decryptable by a unique decryption key unique to said data reproduction unit,

wherein said data reproduction unit comprises

a key hold unit (1540) prestoring said unique decryption key,

a first decryption processing unit (1530) decrypting for said unique decryption key said first session key encrypted in a form decryptable with said unique decryption key supplied from said data storage unit for extraction,

a session key generation unit (1552) generating a second session key updated for every access to obtain said content key with respect to said data storage unit,

a first encryption processing unit (1554) encrypting and providing to said data storage unit said second session key by said first session key,

a second decryption processing unit (1556) decrypting for said second session key said content data supplied from said data storage unit in an encrypted form with said second session key, and

a third decryption processing unit (1520) receiving said encrypted content data supplied from said data storage unit based on an output of said second decryption processing unit to extract content data.

35. The data reproduction apparatus according to claim 34, further comprising an authentication data hold unit (1560) storing, in an encrypted form decryptable by an authentication key, a public encryption key that is an encryption key unique to said data reproduction unit and directed to apply encryption that is decryptable with said unique decryption key and authentication data unique to said data reproduction unit, and that can output the stored public encryption key and authentication data to said data storage unit.

36. The data reproduction apparatus according to claim 35, wherein said data storage unit is detachable with respect to said data reproduction apparatus.

37. The data reproduction apparatus according to claim 34, wherein said content key is stored in said recording unit in an encrypted form decryptable with a predetermined second decryption key by said data reproduction apparatus,

wherein said data reproduction unit further comprises a fifth decryption processing unit (1572) to carry out decryption using a predetermined second decryption key,

wherein said fifth decryption processing unit receives as a decrypted result for said second session key by said second decryption processing unit said content key supplied from said data storage unit in an encrypted form decryptable with said second decryption key and further encrypted with said second session key, and decrypting said content key for said second decryption key to provide the decrypted content key to said third decryption processing unit.

38. The data reproduction apparatus according to claim 34, wherein said data storage unit is detachable with respect to said data reproduction apparatus.

39. The data reproduction apparatus according to claim 34, further comprising an interface for connection to a portable telephone network.

40. The data reproduction apparatus according to claim 39, further comprising a conversation processing unit to carry out conversation via said interface.

41. The data reproduction apparatus according to claim 34, wherein said data storage unit is a memory card detachable with respect to said data reproduction unit.

42. The data reproduction apparatus according to claim 34, wherein said data reproduction unit has at least said key hold unit, said first decryption processing unit, said second decryption processing unit and said third decryption processing unit provided in a security region that cannot be read out by a third party.

43. The data reproduction apparatus according to claim 34, wherein said data storage unit (150, 160) comprises

a recording unit (1412) to store data applied to said data storage unit,

a second session key generation unit (1450) generating said first session key,

a second encryption processing unit (1452) encrypting said first session key generated at said second session key generation unit by a public encryption key unique to said content data reproduction unit and directed to apply encryption that can be decrypted with said unique decryption key,

a fourth decryption processing unit (154) to decrypt, using said first session key, said second session key transmitted from said data reproduction unit in an encrypted form with said first session key, and

a third encryption processing unit (1456) applying an encryption process by said second session key extracted at said fourth decryption processing unit for output,

wherein said content key stored in said recording unit is encrypted at said third encryption processing unit and supplied to said data reproduction unit.

44. The data reproduction apparatus according to claim 35, wherein said data storage unit (150, 160) comprises

a recording unit (1412) to store data applied to said data storage unit,

a fourth decryption processing unit (1460) decrypting using an authentication key said public encryption key and said authentication data that are in an encrypted form decryptable by said authentication key to extract said public encryption key and said authentication data,

a control unit (1420) providing control of an authentication process determining whether said content key is to be output or not to a data reproduction unit from which said authentication data is output based on said authentication data extracted at said fourth decryption processing unit,

a second session key generation unit (1450) generating said first session key,

a second encryption processing unit (1452) encrypting said first session key generated at said second session key generation unit by said public encryption key extracted at said fourth decryption, using said first session key, processing unit,

a fourth decryption processing unit (1454) to decrypt said second session key transmitted from said data reproduction unit in an encrypted form with said first session key, and

a third encryption processing unit (1456) carrying out an encryption process with said second session key extracted at said fourth decryption processing unit for output,

wherein said content key stored in said recording unit is encrypted at said third encryption processing unit to be supplied to said data reproduction unit.

45. A data reproduction module (1500) to be loaded in a data reproduction apparatus decrypting encrypted content data to reproduce content data, comprising:

a first key hold unit (1540) prestoring a first decryption key unique to said data reproduction module,

a first decryption processing unit (1530) decrypting for said first decryption key a first session key supplied from a source external to said data reproduction module in an encrypted form that can be decrypted with said second decryption key for every access to obtain a content key which is a decryption key directed to decrypt said encrypted content data, and extracting said decrypted first session key,

a session key generation unit (1552) generating a second session key updated for every access to obtain said content key with respect to a source external to said data reproduction module,

an encryption processing unit (1554) encrypting said second session key using said first session key for output to an external source to said data reproduction module,

a second decryption processing unit (1556) using said second session key to decrypt said content key encrypted with said second session key and supplied from an external source to said data reproduction module, and

a third decryption processing unit (1520) receiving and decrypting said encrypted content data supplied from an external source to said data reproduction module, based on an output of said second decryption processing unit to extract content data.

46. The data reproduction module according to claim 45, further comprising an authentication data hold unit (1560) storing a public encryption key unique to said data reproduction module and which is an encryption key that can be decrypted with said first decryption key and authentication data unique to said data reproduction module in an encrypted form that can be decrypted by an authentication key at an external source to said data reproduction module, and that can output the stored public encryption key and authentication data to an external source to said data reproduction module.

47. The data reproduction module according to claim 45, wherein said content key is input from an external source to said data reproduction module in an encrypted form with said second session key, and said second decryption processing unit (1556) provides a decrypted result to said third decryption processing unit (1520) as a content key directed to decrypt said encrypted content data.

48. The data reproduction module according to claim 45, wherein said content key is input from an external source to said data reproduction module in an encrypted form decryptable with said first decryption key, and further encrypted with said second session key,

wherein said first decryption processing unit decrypts using said first decryption key a content key in an encrypted form decryptable with said first decryption key which is an output of said second decryption processing unit (1556) to extract and provide to said third decryption processing unit (1520) said content key.

49. The data reproduction module according to claim 45, wherein said content key is input from an external source to said data reproduction module in an encrypted form that can be decrypted with said second decryption key, and encrypted with said second session key,

wherein said data reproduction module further comprises

a second key hold unit (1570) prestoring said second decryption key, and

a fourth decryption processing unit (1572) using said second decryption key to decrypt said content key subjected to encryption that can be decrypted with said second decryption key output from said second decryption processing unit (1556) to extract and provide to said third decryption processing unit (1520) said content key.

50. The data reproduction module according to claim 45, wherein said content data is coded data coded with a coding scheme to reduce an amount of data,

said data reproduction module further comprising a decoding unit (1808) reproducing data based on said coding scheme from said coded data.

51. The data reproduction module according to claim 45, wherein said content data is coded audio data coded with a coding scheme to reduce an amount of data,

said data reproduction module further comprising:

an audio decoding unit (1808) reproducing audio data based on said coding scheme from said coded audio data, and

a digital-analog converter (1512) converting said reproduced audio data into analog signals.

52. The data reproduction module according to claim 45, wherein said data reproduction module is a tamper resistance module.

53. A data reproduction apparatus (300, 400, 500, 600) to be loaded with a data recording apparatus (130, 140, 150, 160) storing encrypted content data and a content key which is a decryption key directed to decrypt said encrypted content data to obtain content data, and encrypting a first session key differing for every access to obtain said encrypted content data into a form decryptable with a unique decryption key unique to said data reproduction apparatus, said data reproduction apparatus reproducing said encrypted content data stored in said data recording apparatus using a content key stored in said data recording apparatus, comprising:

a first interface (1200) to attach said data recording apparatus and carry out data transfer with said data recording apparatus,

a key hold unit (1540) prestoring a unique key unique to said data reproduction apparatus,

a first decryption processing unit (1530) using said unique decryption key to decrypt a first session key updated for every access to obtain said content key and supplied from said data recording apparatus in an encrypted form that can be decrypted with said unique decryption key unique to said data reproduction apparatus,

a session key generation unit (1552) generating a second session key updated for every access to obtain said encrypted content key with respect to said data recording apparatus,

an encryption processing unit (1554) encrypting said second session key using said first session key to supply said encrypted session key to said data recording apparatus,

a second decryption processing unit (1556) using said second session key to decrypt said content key encrypted with said second session key and supplied from said data recording apparatus,

a third decryption processing unit (1520) receiving and decrypting said encrypted content data read out from said data recording apparatus based on an output of said second decryption processing unit to extract content data.

54. The data reproduction apparatus according to claim 53, further comprising an authentication data hold unit (1560) storing a public encryption key which is an encryption key unique to said data reproduction apparatus and decryptable with said first decryption key and authentication data unique to said data reproduction apparatus in an encrypted form that can be decrypted by an authentication key at said data recording apparatus, and providing the stored public encryption key and authentication data to said data recording apparatus.

55. The data reproduction apparatus according to claim 53, wherein said content key is encrypted with said second session key and supplied from said data recording apparatus (150), and said second decryption processing unit (1556) provides a decrypted result to said third decryption processing unit (1520) as a content key directed to decrypt said encrypted content data.

56. The data reproduction apparatus according to claim 53, wherein said content key is encrypted in a form decryptable with said first decryption key, and encrypted with said second session key to be supplied from said data recording apparatus (130, 140),

wherein said first decryption processing unit uses said first decryption key to decrypt an encrypted content key that can be decrypted with said first decryption key which is an output of said second decryption processing unit (1556) to extract and provide to said third decryption processing unit (1520) said content key.

57. The data reproduction apparatus according to claim 53, wherein said content key is encrypted in a form decryptable with said second decryption key, and encrypted with said second session key to be supplied from said data recording apparatus (160),

said data reproduction apparatus further comprising:

a second key hold unit (1570) prestoring said second decryption key, and

a fourth decryption processing unit (1572) using said second decryption key to decrypt said content key in an encrypted form decryptable with said second decryption key output from said

second decryption processing unit (1556) to extract and provide to said third decryption processing unit (1520) said content key.

58. The data reproduction apparatus according to claim 53, wherein said content data is coded data encoded by a coding scheme to reduce an amount of data,

said data reproduction apparatus further comprising a decoding unit (1808) reproducing data based on said coding scheme from said coded data.

59. The data reproduction apparatus according to claim 53, wherein said content data is coded audio data coded by a coding scheme to reduce an amount of data,

said data reproduction apparatus comprising:

an audio decoding unit (1808) reproducing audio data based on said coding scheme from said coded audio data, and

a digital-analog converter (1512) converting said reproduced audio data into analog signals.

60. The data reproduction apparatus according to claim 53, further comprising a second interface connected to a portable telephone network.

61. The data reproduction apparatus according to claim 60, further comprising a conversation processing unit to carry out conversation via said second interface.

62. The data reproduction apparatus according to claim 53, said data reproduction apparatus comprising a security region that cannot be read out by a third party,

wherein at least said first key hold unit, said first decryption processing unit, said second decryption processing unit and said third decryption processing unit are provided in said security region.

63. The data reproduction apparatus according to claim 53, said data reproduction apparatus including a security region that cannot be read out by a third party,

wherein at least said first key hold unit, said second key hold unit, said first decryption processing unit, said second decryption processing unit, said third decryption processing unit, and said second decryption processing unit are provided in said security region.

Masayuki HATANAKA et al. Docket No. 020234

REMARKS

The above amendments are submitted to place the specification and claims in substantially the same conditions as to the claims which have been amended under Article 34 in the international application. An English translation of the annexes of the PCT international preliminary examination report is enclosed. Early and favorable action is awaited.

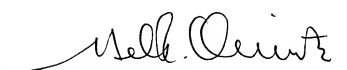
As to the re-numbering of the claims, added claims 23-44 correspond to claims 1-22, respectively, as amended in the international application, while added claims 45-63 correspond to claims 23-41, respectively, as added in the international application.

Attached hereto is a marked-up version of the changes made to the title of the specification by the current amendment. The attached page is captioned "Version with markings to show changes made."

In the event there are any additional fees required, please charge our Deposit Account No. 01-2340.

Respectfully submitted,

ARMSTRONG, WESTERMAN & HATTORI, LLP



Mel R. Quintos
Reg. No. 31,898

Atty. Docket No. 020234
Suite 1000
1725 K Street, N.W.
Washington, D.C. 20006
Tel: (202) 659-2930
MRQ/yap
Enclosures: English translation of the Annexes

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE TITLE:

The title of the specification has been amended as follows:

DATA REPRODUCTION APPARATUS AND DATA REPRODUCTION MODULE

DESCRIPTION

Data Reproduction Apparatus and Data Reproduction Module

Technical Field

The present invention relates to a reproduction apparatus of data distributed through a data distribution system such as a cellular phone network. More particularly, the present invention relates to a data reproduction apparatus that allows protection on copyrights with respect to distributed data.

Background Art

By virtue of the progress in information communication networks and the like such as the internet in these few years, each user can now easily access network information through individual-oriented terminals employing a cellular phone or the like.

In such information communication, information is transmitted through digital signals. It is now possible to obtain copied audio data and image data transmitted via the aforementioned information communication network without almost no degradation in the audio quality and picture quality of the copied data, even in the case where the copy operation is performed by an individual user.

Thus, there is a possibility of the copyright of the copyright owner being significantly infringed unless some appropriate measures to protect copyrights are taken in the case where any created work subject to copyright protection such as audio data and image data is to be transmitted on such an information communication network.

However, if copyright protection is given top priority so that distribution of copyrighted data through the disseminating digital information communication network is suppressed, the copyright owner who can essentially collect a predetermined copyright royalty for copies of a copyrighted work will also incur some disbenefit.

In the case where copyrighted data such as audio data is distributed

through the above-described digital information communication network, each user will reproduce the distributed data using a reproduction apparatus after the distributed data is recorded on some recording device.

Such a recording device includes, for example, a medium that allows data to be written and erased electrically such as a memory card.

As the apparatus to reproduce the distributed data, the cellular phone per se used to receive data distribution can be employed. Alternatively, in the case where the recording device is detachable from the apparatus that receives distribution such as a memory card, a dedicated reproduction apparatus can be used.

In such a case, some security measures must be taken at the recording medium side in order to protect the rights of the copyright owner so that content data (audio data or the like) received by distribution cannot be transferred illegally to another record medium without the permission of the copyright owner.

Furthermore, protection on the rights of the copyright owner and the proper user will be impaired if one other than the user who has received content data distribution by appropriately paying the proper price can freely read out the content data at the reproduction apparatus side during the reproduction of audio data and the like from the recording medium.

Disclosure of the Invention

An object of the present invention is to provide a data reproduction apparatus with the capability of preventing any unauthorized user from accessing copyrighted data such as audio data distributed and stored in a recording device in the reproduction apparatus that reproduces copyrighted data.

To achieve the above object, a data reproduction apparatus of the present invention decrypts encrypted content data to reproduce the content data, and includes a data reproduction unit and a data storage unit.

The data reproduction unit reproduces encrypted content data. The data storage unit stores encrypted content data and an encrypted content key that corresponds to a content key directed to decrypt the encrypted

content data and encrypted in a form decryptable by a first decryption key unique to the data reproduction unit, and outputs the stored content data and content key to the data reproduction unit.

The data reproduction unit includes a session key generation unit, a first encryption processing unit, a first decryption processing unit, a first key hold unit, a second decryption processing unit, and a third decryption processing unit.

The session key generation unit generates a session key updated at every access to obtain a content key with respect to the data storage unit. The first encryption processing unit encrypts the session key using a public encryption key that is decryptable at the data storage unit and unique to the data storage unit, and provides the encrypted key to the data storage unit. The first decryption processing unit uses the session key to decrypt the encrypted content key obtained from the data storage unit in a form encrypted by the session key.

The first key hold unit prestores a first decryption key. The second decryption processing unit extracts a content key by applying a decryption process on the output from the first decryption processing unit using the first decryption key stored in the first key hold unit. The third decryption processing unit receives and decrypts the encrypted content data read out from the data storage unit using the content key extracted by the second decryption processing unit to extract content data.

According to another aspect of the present invention, a data reproduction apparatus decrypts encrypted content data to reproduce content data, and includes a data reproduction unit and a data storage unit.

The data reproduction unit decrypts the encrypted content data using a content key directed to decrypt encrypted content data to reproduce the content data. The data storage unit stores encrypted content data and a content key, and supplies to the data reproduction unit a first session key that differs for every access to obtain a content key and encrypted in a form that is decryptable by a unique decryption key unique to the data reproduction unit,.

The data reproduction unit includes a first key hold unit, a first

decryption processing unit, a first session key generation unit, a first encryption processing unit, a second decryption processing unit and a third decryption processing unit.

The first key hold unit prestores a unique decryption key. The first decryption processing unit applies a decryption process using a unique decryption key which is output from the first key hold unit. The first session key generation unit generates a second session key that is updated for every access to obtain a content key with respect to the data storage unit. The first encryption processing unit uses a first session key that is encrypted in a form decryptable with a unique decryption key supplied from the data storage unit and decrypted at the first decryption processing unit to encrypt and apply to the data storage unit a second session. The second decryption processing unit decrypts for the second session key the content key supplied from the data storage unit after being encrypted in a form decryptable with a unique decryption key and further encrypted with the second session key. The first decryption processing unit extracts the content key by further applying a decryption process on the output from the second decryption processing unit using a unique decryption key. The third decryption processing unit receives the encrypted content data supplied from the data storage unit and applies decryption using the content key extracted by the first decryption processing unit to extract content data.

According to a further aspect of the present invention, a data reproduction apparatus decrypts encrypted content data to reproduce content data, and includes a data reproduction unit and a data storage unit.

The data reproduction unit decrypts the encrypted content data using a content key directed to decrypt the encrypted content data to reproduce the content data. The data storage unit stores encrypted content data and a content key, and supplies to the data reproduction unit a first session key that differs for every access to obtain the encrypted content key and that is encrypted in a form decryptable by a unique decryption key unique to the data reproduction unit.

The data reproduction unit includes a key hold unit, a first

decryption processing unit, a session key generation unit, a first encryption processing unit, a second decryption processing unit and a third decryption processing unit.

The key hold unit prestores a unique decryption key. The first decryption processing unit decrypts for a unique decryption key a first session key that is encrypted in a form decryptable by the unique decryption key supplied from the data storage unit to extract the first session key. The session key generation unit generates a second session key updated for every access to obtain a content key with respect to the data storage unit. The first encryption processing unit encrypts the second session key with the first session key and provides the encrypted session key to the data storage unit. The second decryption processing unit decrypts for the second session key the content key supplied from the data storage unit in an encrypted form with the second session key. The third decryption processing unit receives the encrypted content data supplied from the data storage unit to apply decryption based on the output of the second decryption processing unit to extract content data.

According to a further aspect of the present invention, a data reproduction module to be incorporated in a data reproduction apparatus decrypting encrypted content data to reproduce content data includes a first key hold unit, a first decryption processing unit, a session key generation unit, an encryption processing unit, a second decryption processing unit and a third decryption processing unit.

The first key hold unit prestores a first decryption key unique to the data reproduction module. The first decryption processing unit decrypts for a first decryption key a first session key supplied from an external source to the data reproduction module in an encrypted form that is decryptable by a second decryption key for every access to obtain a content key which is the decryption key directed to decrypt encrypted content data and extracts the first session key. The session key generation unit generates a second session key updated for every access to obtain a content key with respect to an external source to the data reproduction module. The encryption processing unit encrypts the second session key using the

first session key and applies the encrypted session key to an external source to the data reproduction module. The second decryption processing unit decrypts using the second session key the content key encrypted using the second session key and supplied external to the data reproduction module. The third decryption processing unit receives and decrypts the encrypted content data supplied from an external source to the data reproduction module based on the output of the second decryption processing unit to extract content data.

According to still another aspect of the present invention, a data reproduction apparatus is loaded with a data recording apparatus that stores encrypted content data and a content key which is a decryption key directed to decrypt the encrypted content data to obtain content data, and that encrypts a first session key differing for every access to obtain encrypted content data into a form decryptable with a unique decryption key unique to the data reproduction apparatus to supply the encrypted first session key to the data reproduction apparatus. The data reproduction apparatus reproduces encrypted content data stored in the data recording apparatus using the encrypted content key stored in the data recording apparatus, and includes a first interface, a key hold unit, a first decryption processing unit, a session key generation unit, an encryption processing unit, a second decryption processing unit, and a third decryption processing unit.

The first interface serves to attach the data recording apparatus and effect data transfer with the data recording apparatus. The key hold unit prestores a unique key unique to the data reproduction apparatus. The first decryption processing unit decrypts for a unique decryption key a first session key that is updated for every access to obtain a content key and supplied from the data recording apparatus in an encrypted form that is decryptable by a unique decryption key unique to the data reproduction apparatus to extract the first session key. The session key generation unit generates a second session key updated for every access to obtain an encrypted content key with respect to the data recording apparatus. The encryption processing unit encrypts the second session key using the first

session key and provides the encrypted session key to the data recording apparatus. The second decryption processing unit uses the second session key to decrypt the content key supplied from the data recording apparatus in an encrypted form with the second session key. The third decryption processing unit receives and decrypts the encrypted content data read out from the data recording apparatus based on the output of the second decryption processing unit to extract content data.

According to the data reproduction apparatus of the present invention, it is difficult for a third party to improperly access distribution data as to content data stored in a memory by a proper user. It is therefore possible to prevent the copyright owner or proper user from incurring disbenefit by an improper process carried out without permission.

Brief Description of the Drawings

Fig. 1 is a schematic diagram to describe an entire structure of an information distribution system of the present invention.

Fig. 2 is a schematic block diagram to describe a structure of a cellular phone 100 of Fig. 1.

Fig. 3 is a flow chart to describe a reproduction process to reproduce music from encrypted content data in cellular phone 100.

Fig. 4 is a schematic block diagram to describe a structure of a cellular phone 200 according to a second embodiment of the present invention.

Fig. 5 is a diagram to describe together the characteristics of key data and the like for communication used in cellular phone 200 of Fig. 4.

Fig. 6 is a schematic block diagram to describe a structure of a memory card 120 shown in Fig. 4.

Fig. 7 is a flow chart to describe a reproduction process to reproduce

Translation of Annexes to IPER
(SUBSTITUTE SHEET)

CLAIMS

1. (Amended) A data reproduction apparatus (200) decrypting encrypted content data to reproduce content data, comprising:

a data reproduction unit (1500) to reproduce said encrypted content data, and

a data storage unit (120) storing said encrypted content data and an encrypted content key that is a content key directed to decrypt said encrypted content data in an encrypted form decryptable with a first decryption key unique to said data reproduction unit, and providing said encrypted content data and said encrypted content key to said data reproduction unit,

wherein said data reproduction unit comprises

a session key generation unit (1520) generating a session key updated at every access to obtain said content key with respect to said data storage unit,

a first encryption processing unit (1540) encrypting said session key using a public encryption key that can be decrypted at said data storage unit and that is unique to said data storage unit, and providing said encrypted session key to said data storage unit,

a first decryption processing unit (1506) using said session key to decrypt said encrypted content key obtained from said data storage unit in an encrypted form with said session key,

a first key hold unit (1540) prestoring said first decryption key,

a second decryption processing unit (1530) extracting said content key by applying a decryption process on an output from said first decryption processing unit using said first decryption key stored in said first key hold unit, and

a third decryption processing unit (1520) receiving said encrypted content data read out from said data storage unit to decrypt said encrypted content data using a content key extracted by said second decryption processing unit to extract content data.

2. (Amended) The data reproduction apparatus according to claim 1, said content data being coded audio data coded according to a coding scheme to reduce an amount of data,

wherein said data reproduction unit comprises

an audio decoding unit (1508) reproducing audio data based on said coding scheme from said coded audio data, and

a digital-analog converter (1512) converting said reproduced audio data into an analog signal.

3. (Amended) The data reproduction apparatus according to claim 1, wherein said data reproduction unit is provided in a security region that cannot be read out by a third party.

4. (Amended) The data reproduction apparatus according to claim 1, wherein said data storage unit (120) comprises

a record unit (1412) to store data applied to said data storage unit,

a second key hold unit (1401) storing said public encryption key unique to said data storage unit, and that can supply said public encryption key to said data reproduction unit,

a third key hold unit (1402) storing a second decryption key used to decrypt data encrypted with said public encryption key,

a fourth decryption processing unit (1404) using said second decryption key to decrypt said first session key transmitted from said data reproduction unit in an encrypted form by said public encryption key, and

a second encryption processing unit (1406) encrypting encrypted content key stored in said recording unit using said first session key extracted at said fourth decryption processing unit for output.

5. (Amended) The data reproduction apparatus according to claim 1, wherein said data storage unit is detachable with respect to said data reproduction unit.

6. (Amended) A data reproduction apparatus (300, 400)

decrypting encrypted content data to reproduce content data, comprising:

a data reproduction unit (1500) decrypting said encrypted content data using a content key directed to decrypt said encrypted content data to reproduce content data, and

a data storage unit (130, 140) storing said encrypted content data and said content key, and encrypting a first session key differing for every access to obtain said content key into a form decryptable by a unique decryption key unique to said data reproduction unit for supply to said data reproduction unit,

wherein said data reproduction unit comprises

a first key hold unit (1540) prestoring said unique decryption key,

a first decryption processing unit (1530) applying a decryption processing using said unique decryption key which is an output from said first key hold unit,

a first session key generation unit (1522) generating a second session key updated for every access to obtain said content key with respect to said data storage unit,

a first encryption processing unit (1554) encrypting and applying to said data storage unit said second session key using a first session key that is encrypted in a form decryptable with said unique decryption key supplied from said data storage unit and decrypted at said first decryption processing unit, and

a second decryption processing unit (1556) decrypting for said second session key said content key supplied from said data storage unit in an encrypted form decryptable by said unique decryption key and further encrypted with said second session key,

said first decryption processing unit extracting said content key by applying a further decryption process on the output from said second decryption processing unit using said unique decryption key,

wherein said data reproduction unit further comprises a third decryption processing unit (1520) receiving said encrypted content data supplied from said data storage unit to decrypt said receive encrypted content data using a content key extracted by said first decryption

processing unit to extract content data.

7. (Amended) The data reproduction apparatus according to claim 6, wherein said content data is coded audio data encoded by a coding scheme to reduce an amount of data,

wherein said data reproduction unit further comprises

an audio decoding unit reproducing audio data based on said coding method from said coded audio data, and

a digital-analog converter converting said reproduced audio data into an analog signal.

8. (Amended) The data reproduction apparatus according to claim 7, wherein said data reproduction unit has at least said first key hold unit, said first decryption processing unit, said second decryption processing unit and said third decryption processing unit provided in a security region that cannot be read out by a third party.

9. (Amended) The data reproduction apparatus according to claim 6, wherein said data storage unit (130, 140) comprises

a recording unit (1412) to store data applied to said data storage unit,

a second session key generation unit (1450) generating said first session key,

a second encryption processing unit (1452) applying an encryption process using a public encryption key unique to said data reproduction unit and directed to apply encryption that can be decrypted with said unique decryption key,

a fourth decryption processing unit (1454) using said first session key to decrypt said second session key transmitted from said data reproduction unit in an encrypted form with said first session key, and

a third encryption processing unit (1456) carrying out an encryption process by said first session key extracted at said fourth decryption processing unit for output,

said content key stored in said recording unit being encrypted at said

second encryption processing unit and further encrypted at said third encryption processing unit to be supplied to said data reproduction unit.

10. (Amended) The data reproduction apparatus according to claim 6, wherein said data storage unit is a memory card detachable with respect to said data reproduction unit.

11. (Amended) The data reproduction apparatus according to claim 9, further comprising an authentication data hold unit (1560) storing and supplying to said data storage unit authentication data unique to said data reproduction unit together with said public encryption key in an encrypted form decryptable by an authentication key at said data storage unit,

wherein said data storage unit (140) comprises

a fifth decryption processing unit (1460) decrypting and extracting said authentication data and said public encryption key applied from said data reproduction unit in an encrypted form by said authentication key, and

control means carrying out an authentication process to determine whether to output said content key to a data reproduction unit from which said authentication data is output based on said authentication data extracted by said fifth decryption processing unit.

12. (Amended) A data reproduction apparatus (500, 600) decrypting encrypted content data to reproduce content data, comprising:

a data reproduction unit decrypting said encrypted content data using a content key directed to decrypt said encrypted content data to reproduce content data, and

a data storage unit (150, 160) storing said encrypted content data and said content key, and encrypting and supplying to said data reproduction unit a first session key differing for every access to obtain said encrypted content data in an encrypted form decryptable by a unique decryption key unique to said data reproduction unit,

wherein said data reproduction unit comprises

a key hold unit (1540) prestoring said unique decryption key,

a first decryption processing unit (1530) decrypting for said unique decryption key said first session key encrypted in a form decryptable with said unique decryption key supplied from said data storage unit for extraction,

a session key generation unit (1552) generating a second session key updated for every access to obtain said content key with respect to said data storage unit,

a first encryption processing unit (1554) encrypting and providing to said data storage unit said second session key by said first session key,

a second decryption processing unit (1556) decrypting for said second session key said content data supplied from said data storage unit in an encrypted form with said second session key, and

a third decryption processing unit (1520) receiving said encrypted content data supplied from said data storage unit based on an output of said second decryption processing unit to extract content data.

13. (Amended) The data reproduction apparatus according to claim 12, further comprising an authentication data hold unit (1560) storing, in an encrypted form decryptable by an authentication key, a public encryption key that is an encryption key unique to said data reproduction unit and directed to apply encryption that is decryptable with said unique decryption key and authentication data unique to said data reproduction unit, and that can output the stored public encryption key and authentication data to said data storage unit.

14. (Amended) The data reproduction apparatus according to claim 13, wherein said data storage unit is detachable with respect to said data reproduction apparatus.

15. (Amended) The data reproduction apparatus according to claim 12, wherein said content key is stored in said recording unit in an

encrypted form decryptable with a predetermined second decryption key by said data reproduction apparatus,

wherein said data reproduction unit further comprises a fifth decryption processing unit (1572) to carry out decryption using a predetermined second decryption key,

wherein said fifth decryption processing unit receives as a decrypted result for said second session key by said second decryption processing unit said content key supplied from said data storage unit in an encrypted form decryptable with said second decryption key and further encrypted with said second session key, and decrypting said content key for said second decryption key to provide the decrypted content key to said third decryption processing unit.

16. (Amended) The data reproduction apparatus according to claim 12, wherein said data storage unit is detachable with respect to said data reproduction apparatus.

17. (Amended) The data reproduction apparatus according to claim 12, further comprising an interface for connection to a portable telephone network.

18. (Amended) The data reproduction apparatus according to claim 17, further comprising a conversation processing unit to carry out conversation via said interface.

19. (Amended) The data reproduction apparatus according to claim 12, wherein said data storage unit is a memory card detachable with respect to said data reproduction unit.

20. (Amended) The data reproduction apparatus according to claim 12, wherein said data reproduction unit has at least said key hold unit, said first decryption processing unit, said second decryption processing unit and said third decryption processing unit provided in a

security region that cannot be read out by a third party.

21. (Amended) The data reproduction apparatus according to claim 12, wherein said data storage unit (150, 160) comprises

a recording unit (1412) to store data applied to said data storage unit,

a second session key generation unit (1450) generating said first session key,

a second encryption processing unit (1452) encrypting said first session key generated at said second session key generation unit by a public encryption key unique to said content data reproduction unit and directed to apply encryption that can be decrypted with said unique decryption key,

a fourth decryption processing unit (154) to decrypt, using said first session key, said second session key transmitted from said data reproduction unit in an encrypted form with said first session key, and

a third encryption processing unit (1456) applying an encryption process by said second session key extracted at said fourth decryption processing unit for output,

wherein said content key stored in said recording unit is encrypted at said third encryption processing unit and supplied to said data reproduction unit.

22. (Amended) The data reproduction apparatus according to claim 13, wherein said data storage unit (150, 160) comprises

a recording unit (1412) to store data applied to said data storage unit,

a fourth decryption processing unit (1460) decrypting using an authentication key said public encryption key and said authentication data that are in an encrypted form decryptable by said authentication key to extract said public encryption key and said authentication data,

a control unit (1420) providing control of an authentication process determining whether said content key is to be output or not to a data reproduction unit from which said authentication data is output based on said authentication data extracted at said fourth decryption processing unit,

a second session key generation unit (1450) generating said first session key,

a second encryption processing unit (1452) encrypting said first session key generated at said second session key generation unit by said public encryption key extracted at said fourth decryption, using said first session key, processing unit,

a fourth decryption processing unit (1454) to decrypt said second session key transmitted from said data reproduction unit in an encrypted form with said first session key, and

a third encryption processing unit (1456) carrying out an encryption process with said second session key extracted at said fourth decryption processing unit for output,

wherein said content key stored in said recording unit is encrypted at said third encryption processing unit to be supplied to said data reproduction unit.

23. (Added) A data reproduction module (1500) to be loaded in a data reproduction apparatus decrypting encrypted content data to reproduce content data, comprising:

a first key hold unit (1540) prestoring a first decryption key unique to said data reproduction module,

a first decryption processing unit (1530) decrypting for said first decryption key a first session key supplied from a source external to said data reproduction module in an encrypted form that can be decrypted with said second decryption key for every access to obtain a content key which is a decryption key directed to decrypt said encrypted content data, and extracting said decrypted first session key,

a session key generation unit (1552) generating a second session key updated for every access to obtain said content key with respect to a source external to said data reproduction module,

an encryption processing unit (1554) encrypting said second session key using said first session key for output to an external source to said data reproduction module,

a second decryption processing unit (1556) using said second session key to decrypt said content key encrypted with said second session key and supplied from an external source to said data reproduction module, and

a third decryption processing unit (1520) receiving and decrypting said encrypted content data supplied from an external source to said data reproduction module, based on an output of said second decryption processing unit to extract content data.

24. (Added) The data reproduction module according to claim 23, further comprising an authentication data hold unit (1560) storing a public encryption key unique to said data reproduction module and which is an encryption key that can be decrypted with said first decryption key and authentication data unique to said data reproduction module in an encrypted form that can be decrypted by an authentication key at an external source to said data reproduction module, and that can output the stored public encryption key and authentication data to an external source to said data reproduction module.

25. (Added) The data reproduction module according to claim 23, wherein said content key is input from an external source to said data reproduction module in an encrypted form with said second session key, and said second decryption processing unit (1556) provides a decrypted result to said third decryption processing unit (1520) as a content key directed to decrypt said encrypted content data.

26. (Added) The data reproduction module according to claim 23, wherein said content key is input from an external source to said data reproduction module in an encrypted form decryptable with said first decryption key, and further encrypted with said second session key,

wherein said first decryption processing unit decrypts using said first decryption key a content key in an encrypted form decryptable with said first decryption key which is an output of said second decryption processing unit (1556) to extract and provide to said third decryption processing unit

(1520) said content key.

27. (Added) The data reproduction module according to claim 23, wherein said content key is input from an external source to said data reproduction module in an encrypted form that can be decrypted with said second decryption key, and encrypted with said second session key,

wherein said data reproduction module further comprises

a second key hold unit (1570) prestoring said second decryption key, and

a fourth decryption processing unit (1572) using said second decryption key to decrypt said content key subjected to encryption that can be decrypted with said second decryption key output from said second decryption processing unit (1556) to extract and provide to said third decryption processing unit (1520) said content key.

28. (Added) The data reproduction module according to claim 23, wherein said content data is coded data coded with a coding scheme to reduce an amount of data,

said data reproduction module further comprising a decoding unit (1808) reproducing data based on said coding scheme from said coded data.

29. (Added) The data reproduction module according to claim 23, wherein said content data is coded audio data coded with a coding scheme to reduce an amount of data,

said data reproduction module further comprising:

an audio decoding unit (1808) reproducing audio data based on said coding scheme from said coded audio data, and

a digital-analog converter (1512) converting said reproduced audio data into analog signals.

30. (Added) The data reproduction module according to claim 23, wherein said data reproduction module is a tamper resistance module.

31. (Added) A data reproduction apparatus (300, 400, 500, 600) to be loaded with a data recording apparatus (130, 140, 150, 160) storing encrypted content data and a content key which is a decryption key directed to decrypt said encrypted content data to obtain content data, and encrypting a first session key differing for every access to obtain said encrypted content data into a form decryptable with a unique decryption key unique to said data reproduction apparatus, said data reproduction apparatus reproducing said encrypted content data stored in said data recording apparatus using a content key stored in said data recording apparatus, comprising:

a first interface (1200) to attach said data recording apparatus and carry out data transfer with said data recording apparatus,

a key hold unit (1540) prestoring a unique key unique to said data reproduction apparatus,

a first decryption processing unit (1530) using said unique decryption key to decrypt a first session key updated for every access to obtain said content key and supplied from said data recording apparatus in an encrypted form that can be decrypted with said unique decryption key unique to said data reproduction apparatus,

a session key generation unit (1552) generating a second session key updated for every access to obtain said encrypted content key with respect to said data recording apparatus,

an encryption processing unit (1554) encrypting said second session key using said first session key to supply said encrypted session key to said data recording apparatus,

a second decryption processing unit (1556) using said second session key to decrypt said content key encrypted with said second session key and supplied from said data recording apparatus,

a third decryption processing unit (1520) receiving and decrypting said encrypted content data read out from said data recording apparatus based on an output of said second decryption processing unit to extract content data.

32. (Added) The data reproduction apparatus according to claim 31, further comprising an authentication data hold unit (1560) storing a public encryption key which is an encryption key unique to said data reproduction apparatus and decryptable with said first decryption key and authentication data unique to said data reproduction apparatus in an encrypted form that can be decrypted by an authentication key at said data recording apparatus, and providing the stored public encryption key and authentication data to said data recording apparatus.

33. (Added) The data reproduction apparatus according to claim 31, wherein said content key is encrypted with said second session key and supplied from said data recording apparatus (150), and said second decryption processing unit (1556) provides a decrypted result to said third decryption processing unit (1520) as a content key directed to decrypt said encrypted content data.

34. (Added) The data reproduction apparatus according to claim 31, wherein said content key is encrypted in a form decryptable with said first decryption key, and encrypted with said second session key to be supplied from said data recording apparatus (130, 140),

wherein said first decryption processing unit uses said first decryption key to decrypt an encrypted content key that can be decrypted with said first decryption key which is an output of said second decryption processing unit (1556) to extract and provide to said third decryption processing unit (1520) said content key.

35. (Added) The data reproduction apparatus according to claim 31, wherein said content key is encrypted in a form decryptable with said second decryption key, and encrypted with said second session key to be supplied from said data recording apparatus (160),

said data reproduction apparatus further comprising:

a second key hold unit (1570) prestoring said second decryption key, and

a fourth decryption processing unit (1572) using said second decryption key to decrypt said content key in an encrypted form decryptable with said second decryption key output from said second decryption processing unit (1556) to extract and provide to said third decryption processing unit (1520) said content key.

36. (Added) The data reproduction apparatus according to claim 31, wherein said content data is coded data encoded by a coding scheme to reduce an amount of data,

said data reproduction apparatus further comprising a decoding unit (1808) reproducing data based on said coding scheme from said coded data.

37. (Added) The data reproduction apparatus according to claim 31, wherein said content data is coded audio data coded by a coding scheme to reduce an amount of data,

said data reproduction apparatus comprising:

an audio decoding unit (1808) reproducing audio data based on said coding scheme from said coded audio data, and

a digital-analog converter (1512) converting said reproduced audio data into analog signals.

38. (Added) The data reproduction apparatus according to claim 31, further comprising a second interface connected to a portable telephone network.

39. (Added) The data reproduction apparatus according to claim 38, further comprising a conversation processing unit to carry out conversation via said second interface.

40. (Added) The data reproduction apparatus according to claim 31, said data reproduction apparatus comprising a security region that cannot be read out by a third party,

wherein at least said first key hold unit, said first decryption

processing unit, said second decryption processing unit and said third decryption processing unit are provided in said security region.

41. (Added) The data reproduction apparatus according to claim 31, said data reproduction apparatus including a security region that cannot be read out by a third party,

wherein at least said first key hold unit, said second key hold unit, said first decryption processing unit, said second decryption processing unit, said third decryption processing unit, and said second decryption processing unit are provided in said security region.

DESCRIPTION

Data Reproduction Apparatus

Technical Field

The present invention relates to a reproduction apparatus of data distributed through a data distribution system such as a cellular phone network. More particularly, the present invention relates to a data reproduction apparatus that allows protection on copyrights with respect to distributed data.

Background Art

By virtue of the progress in information communication networks and the like such as the Internet in these few years, each user can now easily access network information through individual-oriented terminals employing a cellular phone or the like.

In such information communication, information is transmitted through digital signals. It is now possible to obtain copied audio data and image data transmitted via the aforementioned information communication network without almost no degradation in the audio quality and picture quality of the copied data, even in the case where the copy operation is performed by an individual user.

Thus, there is a possibility of the copyright of the copyright owner being significantly infringed unless some appropriate measures to protect copyrights are taken in the case where any created work subject to copyright protection such as audio data and image data is to be transmitted on such an information communication network.

However, if copyright protection is given top priority so that distribution of copyrighted data through the disseminating digital information communication network is suppressed, the copyright owner who can essentially collect a predetermined copyright royalty for copies of a copyrighted work will also incur some disbenefit.

In the case where copyrighted data such as audio data is distributed

through the above-described digital information communication network, each user will reproduce the distributed data using a reproduction apparatus after the distributed data is recorded on some recording device.

Such a recording device includes, for example, a medium that allows data to be written and erased electrically such as a memory card.

As the apparatus to reproduce the distributed data, the cellular phone per se used to receive data distribution can be employed. Alternatively, in the case where the recording device is detachable from the apparatus that receives distribution such as a memory card, a dedicated reproduction apparatus can be used.

In such a case, some security measures must be taken at the recording medium side in order to protect the rights of the copyright owner so that content data (audio data or the like) received by distribution cannot be transferred illegally to another record medium without the permission of the copyright owner.

Furthermore, protection on the rights of the copyright owner and the proper user will be impaired if one other than the user who has received content data distribution by appropriately paying the proper price can freely read out the content data at the reproduction apparatus side during the reproduction of audio data and the like from the recording medium.

Disclosure of the Invention

An object of the present invention is to provide a data reproduction apparatus with the capability of preventing any unauthorized user from accessing copyrighted data such as audio data distributed and stored in a recording device in the reproduction apparatus that reproduces copyrighted data.

To achieve the above object, a data reproduction apparatus of the present invention decrypts encrypted content data to reproduce the content data, and includes a data storage unit and a data reproduction unit.

The data storage unit stores encrypted content data and an encrypted content key that is an encrypted version of the content key used to decrypt the encrypted content data.

The data reproduction unit receives an output from the data storage unit to reproduce encrypted content data. The data reproduction unit includes a first key hold unit, a first decryption processing unit, and a second decryption processing unit.

The first key hold unit stores a first decryption key used to decrypt the encrypted content key read out from the data storage unit. The first decryption processing unit extracts a content key by carrying out a decryption process by the output from the first key hold unit based on the encrypted content key from the data storage unit. The second decryption processing unit receives the encrypted content data read out from the data storage unit to decrypt the data according to the output of the first decryption processing unit to extract content data.

According to the data reproduction apparatus of the present invention, it is difficult for a third party to improperly access distribution data as to content data stored in a memory by a proper user. It is therefore possible to prevent the copyright owner or proper user from incurring disbenefit by an improper process carried out without permission.

Brief Description of the Drawings

Fig. 1 is a schematic diagram to describe an entire structure of an information distribution system of the present invention.

Fig. 2 is a schematic block diagram to describe a structure of a cellular phone 100 of Fig. 1.

Fig. 3 is a flow chart to describe a reproduction process to reproduce music from encrypted content data in cellular phone 100.

Fig. 4 is a schematic block diagram to describe a structure of a cellular phone 200 according to a second embodiment of the present invention.

Fig. 5 is a diagram to describe together the characteristics of key data and the like for communication used in cellular phone 200 of Fig. 4.

Fig. 6 is a schematic block diagram to describe a structure of a memory card 120 shown in Fig. 4.

Fig. 7 is a flow chart to describe a reproduction process to reproduce

music from encrypted content data in cellular phone 200.

Fig. 8 is a schematic block diagram to describe a structure of a cellular phone 300 according to a third embodiment of the present invention.

Fig. 9 is a diagram to describe together characteristics of key data and the like for communication used in cellular phone 300 shown in Fig. 8.

Fig. 10 is a schematic block diagram to describe a structure of memory card 130 shown in Fig. 8.

Fig. 11 is a flow chart to describe a reproduction process to reproduce music from encrypted content data within cellular phone 300.

Fig. 12 is a schematic block diagram to describe a structure of a cellular phone 400 according to a fourth embodiment of the present invention.

Fig. 13 is a diagram to describe together characteristics of key data and the like for communication used in cellular phone 400 shown in Fig. 12.

Fig. 14 is a schematic block diagram to describe a structure of memory card 140 shown in Fig. 12.

Fig. 15 is a flow chart to describe a reproduction process to provide music outside from encrypted content data stored in memory card 140.

Fig. 16 is a schematic block diagram to describe a structure of a cellular phone 500 according to a fifth embodiment of the present invention.

Fig. 17 is a schematic block diagram to describe a structure of memory card 150 shown in Fig. 16.

Fig. 18 is a flow chart to describe a reproduction process to provide music outside from encrypted content data stored in memory card 150.

Fig. 19 is a schematic block diagram to describe a structure of a cellular phone 600 according to a sixth embodiment of the present invention.

Fig. 20 is a diagram to describe together characteristics of key data and the like for communication used in cellular phone 600 shown in Fig. 19.

Fig. 21 is a schematic block diagram to describe a structure of memory card 160 shown in Fig. 19.

Fig. 22 is a flow chart to describe a reproduction process to provide

music outside from encrypted content data stored in memory card 160.

Best Mode for Carrying Out the Invention

Embodiments of the present invention will be described hereinafter with reference to the drawings.

First Embodiment

Entire Structure of System

Fig. 1 is a schematic diagram to describe an entire structure of an information distribution system of the present invention.

The present invention is based on a structure of a data distribution system that distributes encrypted audio data to each user via a cellular phone network. However, it will become apparent from the following description that the present invention is not limited to such a case. Other encrypted copyright information data, for example copyrighted information data such as image data, can be decrypted and converted into plaintext for reproduction.

Here, it is assumed that the cellular phone network also includes simple portable telephone networks such as of PHS (Personal Handy Phone).

Referring to Fig. 1, a distribution server 10 that administers audio data subject to copyright protection encrypts audio data (also called "content data" hereinafter) according to a predetermined cryptographic scheme, and provides the encrypted data to a cellular phone company serving as a distribution carrier 20 to distribute information.

Distribution carrier 20 relays through its own cellular telephone network a distribution request from each user to distribution server 10. In response to the distribution request, distribution server 10 distributes the requested encrypted audio data to the cellular phone of the relevant user via the cellular phone network of cellular phone company 20 to provide the content data.

A user 1, for example, can listen to the audio data reproduced via a headphone 140 or the like connected to cellular phone 100.

Such a distribution server 10 and distribution carrier (cellular phone company) 20 are together generically referred to as a music server 30

hereinafter.

The process of transmitting audio data from such a music server 30 to each cellular phone terminal is referred to as "distribution".

By counting the number of times of distributing audio data of, for example, one song, at distribution carrier 20, and collecting the copyright fee incurred every time a user receives (downloads) content data in the form of a telephone bill for the cellular phone, the copyright fee of the copyright owner can be ensured.

Furthermore, since distribution of copyrighted data is conducted through a cellular phone network which is a closed system, there is the advantage that measures to protect copyrights can be taken more easily that compared to an open system such as the Internet.

Structure of Distribution Server 10

Referring to Fig. 1, a distribution server 10 includes a distribution information database 304 to store distribution information such as encrypted content data which is an encrypted version of audio data (content data) according to a predetermined scheme, a content key and the like, an account database 302 to store accounting information according to the number of accesses to the audio data for each user, a content key encryption processing unit 316 to encrypt using a public encryption key KPp a content key Kc directed to decrypt encrypted content data, a controller 312 to transmit/receive data to/from distribution information database 304 and account database 302 via a data bus BS1 to control the operation of distribution server 10, and a communication device 350 to transfer data between distribution server 10 and distribution carrier 20 through a communication network.

Specifically, encrypted content data [Dc] Kc corresponding to content data Dc encrypted into a state that can be decrypted using content key Kc which is the decryption key and also content key Kc are output from distribution information database 304. Controller 312 controls content key encryption processing unit 316 so that [Kc] Kp corresponding to content key Kc encrypted using public encryption key KPp is applied to distribution carrier 20 via communication device 350.

Here, the expression [Y] X implies that data Y is data converted into encryption that can be decrypted using a key X. The keys used in the encryption process and decryption process are also generically referred to as "key".

Structure of Terminal (Cellular Phone)

Fig. 2 is a schematic block diagram to describe a structure of a cellular phone 100 shown in Fig. 1.

Cellular phone 100 includes an antenna 1102 to receive signals transmitted through radio by a cellular phone network, a transmitter/receiver unit 1104 converting received signals from antenna 1102 into baseband signals, or modulating and providing to antenna 1102 the data from a cellular phone, a data bus BS2 to transfer data among each component in cellular phone 100, a controller 1106 with a touch key, a dial key, or the like to control the operation of cellular phone 100 via data bus BS2, a keyboard 1108 to apply a command from an external source to cellular phone 100, a display 1110 to provide the information output from controller 1106 and the like to the user as visual information, and an voice decoding unit 1112 to reproduce audio based on reception data applied via data bus BS2 in a normal conversation mode.

Cellular phone 100 further includes a memory 110 to store encrypted content data [Dc] Kc and encrypted content key [Kc] Kp from server 30, and an audio reproduction module 1500. Audio reproduction module 1500 includes a Kp hold unit 1540 storing a private decryption key Kp, corresponding to a public encryption key KPp, and used to decrypt data encrypted with key KPp, a decryption processing unit 1530 to decrypt using public encryption key KPp transmitted from music server 30 an encrypted content key [Kc] Kp received from memory 110, a decryption processing unit 1520 to decrypt encrypted content data [Dc] Kc distributed from music server 30 and stored in memory 110 using content key Kc that is decrypted and extracted by decryption processing unit 1530, an audio decoding unit 1508 receiving the decrypted content data from decryption processing unit 1520 to reproduce audio data according to a reproduction procedure of the coding scheme used to code the content data, for example the digital

compression coding method such as MP3 (MPEG1 Audio Layer III) and AC3, a combine unit 1510 to receive the output of audio decoding unit 1508 and the output of voice decoding unit 1112 to selectively provide the output or combine the outputs according to the operation mode, and a digital-analog converter 1512 to convert the received output from combine unit 1510 into analog signals for output.

Cellular phone 100 further includes a connection terminal 1514 to receive the output of digital-analog converter 1512 and for connection with a headphone 140.

For the sake of simplification, only the block related to distribution of audio data of the present invention is depicted. The block related to the conversation capability inherent in a cellular phone is partially not illustrated.

According to the structure of Fig. 2, audio decoding unit 1508, Kp hold unit 1540, decryption processing unit 1530 and decryption processing unit 1520 can be incorporated into a module TRM to disable read out by a third party of data and the like in the circuitry residing in the region by erasing internal data or destroying the internal circuitry at an attempt of an improper opening process or the like by an external source. This module is generally referred to as a tamper resistance module.

By such a structure, at least the decryption key and the data in plaintext cannot be looked from an external source. It will become difficult to improperly obtain the encryption scheme and private decryption key of cellular phone 100 from an external source. Therefore, the security is improved.

It is possible to set audio reproduction module 1500 corresponding to the region enclosed by a solid line in Fig. 2 as the TRM. By such a structure, even the eventual digital data of the copyrighted data such as audio data can be protected.

Reproduction Process

Fig. 3 is a flow chart to describe a reproduction process of decrypting content data from the encrypted content data stored in memory 110 to provide music.

Referring to Fig. 3, a reproduction request is applied to controller 1106 in response to a user's command through keyboard 1108 or the like of a cellular phone (step S100).

In response to this reproduction request, controller 1106 controls memory 110 so as to read out encrypted content key [Kc] Kp (step S102).

Then, decryption processing unit 1530 applies a decryption process on encrypted content key [Kc] Kp read out from memory 110 (step S104).

In the case where content key Kc can be decrypted and extracted by decryption processing unit 1530 (step S106), control proceeds to the next step. In the case where determination is made that the content key is not decryptable, the process ends (step S110).

In the case where content key Kc can be decrypted and extracted by decryption processing unit 1530, controller 1108 controls memory 110 so that encrypted content data [Dc] Kc is read out. This encrypted content data [Dc] Kc is applied to decryption processing unit 1520. Decryption processing unit 1520 applies a decryption process using decryption key Kc to generate content data Dc in plaintext. This content data Dc is applied to audio decoding unit 1508. At audio decoding unit 1508, the music signal reproduced based on content data Dc is passed through combine unit 1510 to be converted into an analog signal by digital-analog converter 1512. The converted analog signal is output from connection terminal 1514.

According to the above-described structure, only encrypted content data and an encrypted content key are stored in memory 110 in cellular phone 100 which is a reproduction apparatus. Therefore, even if the stored contents in memory 110 is read out by a third party, the music cannot be reproduced.

It is to be noted that the data applied from memory 110 to decryption processing units 1520 and 1530 are such encrypted data. Therefore, even if the signals on data bus BS2 are read out by a third party, the music cannot be reproduced.

The portion to which audio data in plaintext is transmitted is formed of a tamper resistance module. Therefore, it is not possible to read out the audio data from this area outside to an external source.

According to the structure of cellular phone 100 shown in Fig. 2, protection can be conducted so as to prevent the content data from being copied by unauthorized means for reproduction or distribution.

Second Embodiment

Fig. 4 is a schematic block diagram to describe a structure of a cellular phone 200 according to a second embodiment of the present invention. Fig. 4 is comparable with Fig. 2 of the first embodiment.

The difference in structure of cellular phone 200 from cellular phone 200 of Fig. 2 is set forth below.

Referring to Fig. 4, cellular phone 200 has a structure in which a memory card 120 can be loaded. This detachable memory card 120 functions to receive and store encrypted content data received by cellular phone 200, and apply a predetermined encryption process on the encrypted content data and encrypted content key to provide the processed data and key to audio reproduction module 1500. Accordingly, cellular phone 200 further includes a memory interface 1200 to control data transfer between memory card 1200 and data bus BS2.

In cellular phone 200, the structure of audio reproduction module 1500 differs from that of cellular phone 200.

Specifically, audio reproduction module 1500 of cellular phone 200 includes a session key generation unit 1502 to generate through a random number or the like a session key Ks used to encrypt data transferred on data bus BS2 during the data transfer between memory card 120 and other components in cellular phone 200, an encryption processing unit 1504 to encrypt session key Ks generated by session key generation unit 1502 to provide the encrypted session key onto data bus BS2, a decryption processing unit 1506 decrypting for session key Ks a content key Kc transmitted from memory card 120 through data bus BS2, encrypted with public encryption key KPp and session key Ks for output, a Kp hold unit 1540 storing a private decryption key Kp, corresponding to a public encryption key KPp, and used to decrypt data encrypted with key KPp, a decryption processing unit 1530 receiving the output of decryption processing unit 1506 to decrypt encrypted content key [Kc] Kp using public

encryption key KPp transmitted from memory card 120, a decryption processing unit 1520 to decrypt encrypted content data [Dc] Kc distributed from server 30 and stored in memory card 120 based on content key Kc decrypted and extracted by decryption processing unit 1530, an audio decoding unit 1508 receiving decrypted content data Dc from decryption processing unit 1520 to reproduce audio data distributed from music server 30, a combine unit 1510 receiving the output of audio decoding unit 1508 and the output of voice decoding unit 1112 to selectively output or combine the outputs according to the operation mode, and a digital-analog converter 1512 to convert the received output from combine unit 1510 into an analog signal for output.

The other components in cellular phone 200 are similar in structure to those of cellular phone 100 of the first embodiment. Corresponding components have the same reference characters allotted, and description thereof will not be repeated.

In Fig. 4, only the block related to distribution of the audio data of the present invention is depicted for the sake of simplification. The block related to the conversation feature inherent to a cellular phone is partially not illustrated.

According to the structure of Fig. 4, audio decoding unit 1508, Kp hold unit 1540, decryption processing unit 1530, decryption processing unit 1520, decryption processing unit 1506, encryption processing unit 1504 and Ks generation unit 1502 can be incorporated into a TRM.

By such a structure, it is difficult for a third party to improperly obtain the encryption scheme and private decryption key of cellular phone 200 since the decryption key and data in plaintext cannot be looked from an external source. Therefore, the security is improved.

Furthermore, audio reproduction module 1500 corresponding to the region enclosed by a solid line in Fig. 4 can be set as the TRM. According to the structure, protection can be conducted even on the eventual digital data of the copyrighted content data such as audio data.

Structure of Encryption/Decryption Key

Fig. 5 is a diagram to describe together characteristics of key data

and the like for communication used in cellular phone 200 shown in Fig. 4.

In the structure of Fig. 4, the keys to control data processing in memory card 120 include a public encryption key KPm unique to memory card 120 and a private decryption key Km asymmetric to key KPm and used to decrypt data encrypted with public encryption key KPm.

The expression of key KPm and key Km being asymmetric means that data encrypted using a plurality of public encryption keys KPm can be decrypted using a decryption key Km that is different from key KPm and that cannot be easily obtained by analogy.

Therefore, in the transfer of a session key between memory card 120 and cellular phone 200, these encryption key Km and decryption key KPm will be used as described afterwards.

Additionally, the encryption keys used to maintain secrecy in the data transfer with respect to an external source of the memory card include a public encryption key KPm unique to the reproduction apparatus which is a cellular phone here, a private decryption key Kp asymmetric to key KPp, functioning as a key to control the audio reproduction module, and used to decrypt data encrypted with public encryption key KPp, and a symmetric key Ks generated at a Ks generator 150 for every communication.

Symmetric key Ks is generated by Ks generator 1502 every time access is effected for the transfer of content data between, for example, cellular phone 200 and memory card 120.

In the following, this unit of communication or unit of one access is called "session", and symmetric key Ks is also referred to as "session key".

Session key Ks has a value unique to each communication session, and is under control of audio reproduction module 1500.

With regards to copyrighted data stored in memory card 120, there is a content key Kc which is a symmetric key to encrypt content data (audio data) per se. It is assumed that the encrypted content data is decrypted (converted in plaintext) using this content key Kc.

Content data Dc subject to copyright protection includes, for example, audio data. Data corresponding to the content data that can be decrypted using content key Kc is called encrypted content data [Dc] Kc.

In the case where content key Kc is distributed from distribution server 10 to cellular phone 200, it is assumed that content key Kc is encrypted using at least public encryption key KPp, and stored in memory card 120 as encrypted content key [Kc] Kp.

Structure of Memory Card

Fig. 6 is a schematic block diagram to describe a structure of memory card 120 shown in Fig.4.

Memory card 120 includes a data bus BS3 to send/receive a signal to/from memory interface 1200 via terminal 1202, a KPm hold unit 1401 storing a value of public encryption key KPm and providing public encryption key KPm onto data bus BS3, a Km hold unit 1402 to store a private decryption key Km corresponding to card 120, a decryption processing unit 1404 to extract a session key Ks by applying a decryption process on data applied onto data bus BS3 from memory interface 1200 using private decryption key Km, a memory 1412 receiving and storing content key Kc that is encrypted using public encryption key Kp and encrypted content data [Dc] Kc encrypted using content key Kc, an encryption processing unit 1406 encrypting and providing onto data bus BS3 the output from memory 1412 based on session key Ks extracted by decryption processing unit 1404, and a controller 1420 to control the operation of the memory card 120.

Memory card 120 of Fig. 6 can have a structure that is incorporated into module TRM to disable readout by a third party of data and the like in the circuitry residing in this region by erasing internal data or destroying internal circuitry at an attempt of an improper opening process or the like by an external source.

Reproduction Process

Fig. 7 is a flow chart to describe a reproduction process to decrypt music information from the encrypted content data stored in memory card 120 to output music.

Referring to Fig. 7, in response to a user's command through keyboard 1108 or the like of a cellular phone, a reproduction request is output to memory card 120 (step S200).

In response to this reproduction request, control 1420 in memory card 120 transmits public encryption key KPm from KPm hold unit 1401 to cellular phone 200 via data bus BS3, terminal 1202 and memory interface 1200 (step S202).

Upon receiving key KPm from card 120 in cellular phone 200 (step S204), Ks generation unit 1502 generates a session key Ks (step S206). Encryption processing unit 1504 encrypts session key Ks using key KPm to generate an encrypted session key [Ks] KPm. Encrypted session key [Ks] KPm is transmitted to card 120 via data bus BS2 (step S208).

Memory card 120 receives the generated encrypted session key [Ks] KPm from cellular phone 200. Encrypted session key [Ks] KPm is decrypted using private decryption key Km at decryption processing unit 1404, whereby session key Ks is extracted (step S210).

Then, memory card 120 reads out content key [Kc] Kp from memory 1412 (step S212).

Memory card 120 uses session key Ks extracted from encryption processing unit 1406 to encrypt encrypted content key [Kc] Kp, and applies the further encrypted encryption content key [[Kc] Kp] Ks onto data bus BS2 (step S214).

Decryption processing unit 1506 of cellular phone 200 applies a decryption process on encrypted encryption content key [[Kc] Kp] Ks transmitted from memory card 120 by session key Ks, whereby encrypted content key [Kc] Kp is obtained (step S216).

Decryption processing unit 1530 of cellular phone 200 applies a decryption process on data [Kc] Kp based on key Kp from Kp hold unit 1540 (step S218).

When content key Kc can be extracted by this decryption process of decryption processing unit 1530 (step S220), control proceeds to step S222, otherwise (step S220), the process ends (step S226).

When content key Kc is extracted by the decryption process of decryption processing unit 1530, memory card 120 reads out encrypted content data [Dc] Kc from memory 1412 and provides the same onto data bus BS2 (step S222).

Decryption processing unit 1520 of cellular phone 200 applies a decryption process on encrypted content data [Dc] Kc by the extracted content key Kc to generate content data Dc in plaintext. Audio decoding unit 1508 reproduces content data Dc and applies the reproduced content data Dc to combine unit 1510. Digital-analog converter 1512 converts the received data from combine unit 1510 into an analog signal to output reproduced music. Thus, the process ends (step S226).

By the above-described structure, transmission from memory card 120 to cellular phone 200 is effected to carry out a reproduction operation after the content key has been encrypted based on the session key generated at cellular phone 200.

According to cellular phone 200 of the second embodiment, distribution data is stored in a memory card that is detachable with respect to cellular phone 200. The memory card has to be loaded only when distribution is to be received or reproduction is to be carried out. Therefore, there is the advantage that the convenience as a portable apparatus is not degraded from the standpoint of weight and the like, in addition to the advantage described with reference to cellular phone 200 of the first embodiment.

The data transferred between a cellular phone and a memory card is in an encrypted form using a session key. Therefore, the security with respect to data is improved to allow protection on both the rights of the copyright owner and the user.

Subsequent to distribution, reproduction is allowed by loading the memory card in another reproduction apparatus. Therefore, the degree of freedom as to the usage of audio data for the user is improved.

Third Embodiment

Fig. 8 is a schematic block diagram to describe a structure of a cellular phone 300 according to a third embodiment of the present invention. Fig. 8 is comparable with Fig. 4 corresponding to the second embodiment.

Cellular phone 300 of the third embodiment shown in Fig. 8 differs in structure from cellular phone 2 of the second embodiment as set forth

below.

In Fig. 8, cellular phone 300 can be loaded with a detachable memory card 130 receiving and storing encrypted audio data received by cellular phone 300, and further applying a predetermined encryption process on the encrypted content data and encrypted content key to provide the encrypted content data and encrypted content key that are further encrypted to audio reproduction module 1500 in cellular phone 300.

As will be described afterwards, memory card 130 differs from memory card 120 in that a session key Ks2 is generated by memory card 130 itself.

Furthermore, cellular phone 300 differs from cellular phone 200 in the structure of audio reproduction module 1500.

Specifically, audio reproduction module 1500 of cellular phone 300 includes a session key generation unit 1522 generating, using a random number or the like, a session key Ks1 directed to encrypt data transferred on data bus BS2 for the data transfer between memory card 130 and other components in cellular phone 300, an encryption processing unit 1554 encrypting session key Ks1 generated by session key generation unit 1552 with session key Ks2 from memory card 130 and apply the encrypted session key onto data bus BS2, a decryption processing unit 1556 decrypting for session key Ks1 an encrypted content key Kc that is transmitted from memory card 130 through data bus BS2 and that is encrypted with public encryption key KPp and session key Ks1, and a switch circuit 1550 under control of controller 1106 to apply encrypted session key [Ks2] Kp of memory card 130 transmitted via data bus BS2 or encrypted content key [Kc] Kp output from decryption processing unit 1556 to decryption processing unit 1530 directed to decrypt data encrypted with public encryption key KPp.

Encryption processing unit 1554 receives session key Ks2 of memory card 130 decrypted and extracted from decryption process unit 1530 using private decryption key Kp, and applies an encryption process on session key Ks1 generated by session key generation unit 1552 using session key Ks2.

The remaining component of cellular phone 300 are similar to those of cellular phone 200 of the second embodiment. Corresponding components have the same reference characters allotted, and the description thereof will not be repeated.

For the sake of simplification, only the block related to distribution of audio data of the present invention is depicted in Fig. 8. The block related to the conversation function inherent to a cellular phone is partially not illustrated.

In the structure shown in Fig. 8, audio decoding unit 1508, Kp hold unit 1540, decryption processing unit 1530, decryption processing unit 1520, decryption processing unit 1556, encryption processing unit 1554, session key generation unit 1552 and switch circuit 1550 can be incorporated into the TRM.

By the above-described structure, the decryption key and data converted into plaintext cannot be looked from an external source. It will become difficult to improperly obtain the encryption scheme and private decryption key of cellular phone 300 by a third party. Therefore, the security is improved.

Furthermore, audio reproduction module 1500 corresponding to the region enclosed by a solid line in Fig. 8 can be set as the TRM. In this case, the eventual digital data of content data subjected to copyright protection such as audio data can also be protected.

Structure of Encryption/Decryption Key

Fig. 9 is a diagram to describe together the characteristics of key data for communication employed in cellular phone 300 of Fig. 8.

The key to control data processing in memory card 130 according to the structure of Fig. 8 includes a public encryption key KPm unique to the memory card, a private decryption key Km asymmetric to key KPm and used to decrypt data encrypted with public encryption key KPm, and a session key Ks2 generated by memory card 130 and unique to each session.

In the transfer of a session key between memory card 130 and cellular phone 300, private key Km, decryption key KPm, and session key Ks2 will be employed, as will be described afterwards.

Also, the encryption key to maintain security as to data transfer from an external source to memory card 130 includes a public encryption key KPp unique to the reproduction apparatus which is a cellular phone here, distributed together with the content data at the time of distribution of the content data, and stored in memory card 130 as will be described afterwards, a private decryption key Kp asymmetric to key KPp and used as the key to decrypt data encrypted with key KPp as a control key of audio reproduction module 1500, and a session key Ks1 which is a symmetric key generated by session key generator 1552 for each access.

Session key Ks1 has a value unique to each communication session, and is under control of audio reproduction module 1500.

With regards to copyrighted data recorded in memory card 130, it is assumed that the encrypted content data is decrypted (converted into plaintext) using a content key Kc that is the symmetric key directed to encrypt audio data (content data) per se.

In the case where content key Kc is distributed from distribution server 10 towards cellular phone 300, it is assumed that content key Kc is at least encrypted with public encryption key KPp, and stored in memory card 130 as encrypted content key [Kc] Kp.

Furthermore, it is assumed that content data Dc subject to copyright protection is stored in memory card 130 as encrypted content data [Dc] Kc that can be decrypted using content key Kc.

Structure of Memory Card

Fig. 10 is a schematic block diagram to describe a structure of memory card 130 shown in Fig. 8.

Memory card 130 includes a data bus BS3 to send/receive a signal to/from memory interface 1200 via terminal 1202, a session key generation unit 1450 to generate a session key Ks2 for every session, an encryption processing unit 1452 to encrypt session key Ks2 using public encryption key KPp and providing the encrypted session key onto data bus BS3, a decryption processing unit 1454 to extract session key Ks1 from cellular phone 300 by applying a decryption process on data [Ks1] Ks2 applied onto data bus BS3 from memory interface 1200 using session key Ks2, a memory

1412 receiving and storing via data bus BS3 a public encryption key KPp, a content key [Kc] Kp encrypted with public encryption key KPp and encrypted content data [Dc] Kc encrypted by a content key Kc, an encryption processing unit 1456 to encrypt the output from memory 1412 based on session key Ks1 extracted from decryption processing unit 1454 to provide the encrypted data onto data bus BS3, and a controller 1420 to control the operation of memory card 130.

Memory card 130 of Fig. 10 can be incorporated into module TRM to disable readout by a third party of data and the like in the circuitry residing in this region by erasing internal data or destroying internal circuitry at an attempt of an improper opening process or the like by an external source.

Reproduction Process

Fig. 11 is a flow chart to describe a reproduction process of decrypting music information from encrypted content data stored in memory card 130 for output as music.

Referring to Fig. 11, a reproduction request is output to memory card 130 by a user's command through keyboard 1108 or the like of cellular phone 300 (step S300).

In response to this reproduction request, controller 1420 in memory card 130 causes session key generator 1450 to generate a session key Ks2 (step S302). Under control of controller 1420, encryption processing unit 1452 encrypts session key Ks2 using public encryption key KPp to generate an encrypted session key [Ks2] Kp. This encrypted session key [Ks2] Kp is transmitted to cellular phone 300 via data bus BS3, terminal 1202 and memory interface 100 (step S304).

Upon receiving encrypted session key [Ks2] Kp from memory card 130, decryption processing unit 1530 of cellular phone 300 receives and decrypts encrypted session key [Ks2] Kp via switch circuit 1550 to obtain session key Ks2 (step S306).

Session key generation unit 1552 of cellular phone 300 generates a session key Ks2 (step S308). Encryption processing unit 1554 encrypts this session key Ks1 using session key Ks2 extracted at step S306 to

generate an encrypted session key [Ks1] Ks2. This encrypted session key [Ks1] Ks2 is transmitted to card 130 through data bus BS2 (step S310).

Memory card 130 receives session key [Ks1] Ks2 generated and encrypted by cellular phone 300. Decryption processing unit 1454 applies decryption using session key Ks2 to extract session key Ks1 (step S312).

Then, memory card 130 reads out encrypted content key [Kc] Kp from memory 1412 (step S314). Encryption processing unit 1456 encrypts encrypted content key [Kc] Kp using extracted session key Ks1. The further encrypted content data [[Kc] Kp] Ks1 is applied onto data bus BS2 via data bus BS3 and the like (step S316).

Decryption processing unit 1556 of cellular phone 300 applies a decryption process on further encrypted content key [[Kc] Kp] Ks1 transmitted from memory card 130 using session key Ks1, whereby encrypted content key [Kc] Kp is obtained (step S318).

Decryption processing unit 1530 of cellular phone 300 receives encrypted content key [Kc] Kp via switch circuit 1550 to apply a decryption process on encrypted content key [Kc] Kp based on key Kp from Kp hold unit 1540 (step S320).

When content key Kc can be extracted by the decryption process of decryption processing unit 1530 (step S322), control proceeds to step S324. In the case where content key Kc cannot be extracted (step S322), the process ends (step S330).

When content key Kc is extracted by the decryption process of decryption processing unit 1530, memory card 130 reads out encrypted content data [Dc] Kc from memory 1412. The read out encrypted content data [Dc] Kc is applied onto data bus BS2 via data bus BS3 and the like (step S324).

Decryption processing unit 1520 of cellular phone 300 applies a decryption process on encrypted content data [Dc] Kc using the extracted content key Kc to generate content data Dc in plaintext. Audio decoding unit 1508 reproduces content data Dc and provides the same to combine unit 1510. Digital-analog converter 1512 converts the received data from combine unit 1510 into an analog signal to output the reproduced music

(step S328). Thus, the process ends (step S330).

By the above-described structure, transmission from memory card 130 to cellular phone 300 can be effected to carry out a reproduction operation after encrypted content key [Kc] Kp is encrypted based on session key Ks1 generated at cellular phone 300. Since session key Ks1 is transferred between memory card 130 and cellular phone 300 after encryption with session key Ks2 generated for each session at memory card 130, security is further improved than in the second embodiment. The rights of both the copyright owner and the user can be protected.

According to such a structure, distribution data is stored in memory card that is detachable with respect to cellular phone 300. The memory card has to be loaded only at the time of receiving distribution or carrying out reproduction. Therefore, the convenience as a portable apparatus will not be degraded from the standpoint of weight and the like.

Furthermore, following distribution, reproduction can be carried out by loading the memory card to another reproduction apparatus. Therefore, the degree of freedom of the usage of audio data for the user is improved.

Fourth Embodiment

Fig. 12 is a schematic block diagram to describe a structure of cellular phone 400 according to a fourth embodiment of the present invention. Fig. 12 is comparable with Fig. 8 corresponding to the third embodiment.

Cellular phone 400 of Fig. 4 shown in Fig. 12 differs in structure from cellular phone 300 of the third embodiment as set forth below.

Specifically, referring to Fig. 12, cellular phone 400 has a structure that can be loaded with a detachable memory card 140 to apply the required data to audio reproduction module 1500 in cellular phone 400 after a predetermined encryption process is applied on the stored content data and encrypted content key received by cellular phone 400. Memory card 140 differs from memory card 130 of the third embodiment in that an authentication capability is provided with respect to cellular phone 400, as will be described afterwards.

Furthermore, cellular phone 400 differs from cellular phone 300 in

the structure of audio reproduction module 1500.

Specifically, audio reproduction module 1500 of cellular phone 400 further includes a [KPp, Crtf] KPma hold unit 1560 to realize an authentication function with respect to cellular phone 400 in the data transfer between memory card 140 and other components in cellular phone 400. [KPp, Crtf] KPma hold unit 1560 encrypts using a public decryption key (public authentication key) KPma common to the system a public encryption key KPp unique to the class (type) of cellular phone 400 which is a reproduction apparatus and authentication data Crtf and stores the encrypted public encryption key and authentication data.

The remaining components of cellular phone 400 are similar to those of cellular phone 300 of the third embodiment. Corresponding components have the same reference characters allotted, and the description thereof will not be repeated.

For the sake of simplification, only the block related to distribution of audio data of the present invention is depicted in Fig. 12. The block related to the conversation function inherent to a cellular phone is partially not illustrated.

In the structure of Fig. 12, audio decoding unit 1508, Kp hold unit 1540, decryption processing unit 1530, decryption processing unit 1520, decryption processing unit 1556, encryption processing unit 1554, session key generation unit 1552, switch circuit 1550 and [KPp, Crtf] KPma hold unit 1560 can be incorporated into the TRM.

By such a structure, the authentication data, decryption key and data in plaintext cannot be modified or looked by an external source. It is therefore difficult to improperly obtain the encryption scheme and private decryption key of cellular phone 400 from an external source. Thus, the security is improved.

Also, audio reproduction module 1500 corresponding to the region enclosed by a solid line in Fig. 12 can be set as the TRM. By such a structure, the eventual digital data of data subject to copyright protection such as audio data can be protected.

Structure of Encryption/Decryption Key

Fig. 13 is a diagram to describe together the characteristics of key data for communication used in cellular phone 400 of Fig. 12.

According to the structure shown in Fig. 12, the key used to control data processing in memory card 140 includes a public decryption key KPma common to the system and having the capability of an authentication key, and a session key Ks2 generated by memory card 140 and that is a symmetric key unique to each session.

Furthermore, the encryption key to maintain security as to data transfer with a source external to the memory card includes a public encryption key KPp that is unique to the class of the reproduction apparatus which is a cellular phone here, and stored in [KPp, Crtf] KPma hold unit 1560 in cellular phone 400 in an encrypted form by key KPma, a private decryption key Kp asymmetric to key KPp, and used to decrypt data encrypted with key KPp, and a session key Ks1 which is a symmetric key generated by session key generator 1552 for each access.

Session key Ks1 has a value unique to each communication session, and is under control of audio reproduction module 1500.

Here, "the class of reproduction apparatus" is the category to identify each reproduction apparatus or respective reproduction apparatuses of a particular type (manufacturer, manufacture lot).

With regards to the copyrighted data recorded in memory card 140, it is assumed that the encrypted content data is decrypted (into plaintext) using a content key Kc that is a symmetric key directed to encrypt content data (audio data) itself.

When content key Kc is distributed from distribution server 10 to cellular phone 400, it is assumed that content key Kc is encrypted with at least public encryption key KPp, and stored in memory card 140 as encrypted content key [Kc] Kp.

Furthermore, it is assumed that content data Dc subjected to copyright protection is stored in memory card 140 as encrypted content data [Dc] Kc that can be decrypted using content key Kc.

Structure of Memory Card

Fig. 14 is a schematic block diagram to describe a structure of

memory card 140 shown in Fig. 12.

Memory card 140 differs in structure from memory card 130 of the third embodiment in that a decryption processing unit 1460 is included. Under control of controller 1420, decryption processing unit 1460 applies a decryption process on the data on data bus BS3 using public decryption key KPma to obtain public encryption key KPp and authentication data Crtf from cellular phone 140. Therefore, encryption processing unit 1452 carries out an encryption process based on public encryption key KPp from decryption processing unit 1460.

In memory 1412 of memory card 140 is stored a public decryption key KPma instead of public encryption key KPp stored for memory card 130. Therefore, decryption processing unit 1460 carries out a decryption process based on public decryption key KPma stored in memory 1412.

The remaining components of memory card 140 are similar to those of memory card 130 of the third embodiment. Corresponding components have the same reference characters allotted, and the description thereof will not be repeated.

Memory card 140 of Fig. 14 can be incorporated into module TRM to disable read out by a third party of data and the like in the circuitry residing in this region by erasing internal data or destroying internal circuitry at an attempt of an improper opening process or the like by an external source.

Reproduction Process

Fig. 15 is a flow chart to describe a reproduction process of reproducing music from encrypted content data stored in memory card 140 for output as music in cellular phone 400.

Referring to the flow chart of the reproduction process of Fig. 15, application of a reproduction request (step S400) by a user's command through a keyboard 1108 or the like of cellular phone 400 causes data [KPp, Crtf] KPma to be output to memory card 140 from [KPp, Crtf] KPma hold unit 1560 of cellular phone 400 (step S402).

Decode unit 1460 in memory card 140 decrypts data [KPp, Crtf] KPma to obtain a public encryption key KPp and authentication data Crtf

(step S406). Controller 1420 conducts authentication of cellular phone 400 based on authentication data Crtf (step S406). When cellular phone 400 is a proper apparatus, control proceeds to step S408. When cellular phone 400 is not a proper apparatus, the process ends without carrying out an operation for reproduction (step S434).

When cellular phone 400 is a proper apparatus, session key generation unit 1450 generates session key Ks2 under control of controller 1420 (step S408). Under control of controller 1420, encryption processing unit 1452 encrypts session key Ks2 using public encryption key KPp to generate encryption session key [Ks2] Kp. This encryption session key [Ks2] Kp is transmitted to cellular phone 400 via data bus BS3, terminal 1202 and memory interface 1200 (step S410).

When encrypted session key [Ks2] Kp is received from memory card 140, decryption processing unit 1530 of cellular phone 400 receives via switch circuit 1550 encrypted session key [Ks2] Kp and applies decryption to obtain session key Ks2 (step S412).

Session key generation unit 1552 of cellular phone 400 generates session key Ks1 (step S414). Encryption processing unit 1554 encrypts session key Ks1 using session key Ks2 extracted at step S412 to generate data [Ks1] Ks2. Data [Ks1] Ks2 is transmitted to memory card 140 via data bus BS2 (step S416).

Memory card 140 receives session key [Ks1] Ks2 generated and encrypted by cellular phone 400. Decryption processing unit 1454 decrypts the encrypted session key [Ks1] Ks2 using session key Ks2 to extract session key Ks1 (step 418).

Then, memory card 140 reads out encrypted data [Kc] Kp from memory 1412 (step S420). Encryption processing unit 1456 encrypts encrypted content key [Kc] Kp using extracted session key Ks1 to provide further encrypted content key [[Kc] Kp] Ks1 onto data bus BS2 via data bus BS3 and the like (step S422).

Decryption processing unit 1556 of cellular phone 400 applies a decryption process on further encrypted content key [[Kc] Kp] Ks1 transmitted from memory card 140 using session key Ks1 to obtain

encrypted content key [Kc] Kp (step S424).

Decryption processing unit 1530 of cellular phone 400 receives encrypted content key [Kc] Kp via switch circuit 1550 to apply a decryption process of data [Kc] Kp based on key Kp from Kp hold unit 1540 (step S426).

When decryption processing unit 1530 can extract content key Kc by the decryption process (step S428), control proceeds to step S430, otherwise (step S428), the process ends (step S434).

When content key Kc is extracted by the decryption process of decryption processing unit 1530, memory card 140 reads out encrypted content data [Dc] Kc from memory 1412 and provides encrypted content data [Dc] Kc onto data bus BS2 via data bus BS3 and the like (step S430).

Decryption processing unit 1520 of cellular phone 400 decrypts encrypted content data [Dc] Kc using the extracted content key Kc to generate audio data Dc in plaintext. Audio decoding unit 1508 reproduces content data Dc and provides the reproduced data to combine unit 1510. Digital-analog converter 1512 converts the data received from combine unit 1510 to provide reproduced music outside (step S432). Thus, the process ends (step S434).

By the above-described structure, a reproduction operation is allowed only between memory card 140 and a cellular phone 400 verified as a proper apparatus as a result of authentication by memory card 140 based on data [[KPp, Crtf] KPma from cellular phone 400. Therefore, in addition to the advantages of cellular phone 300 and memory card 130 of the third embodiment, there are the advantages that the security of the system is further improved and the copyright of the copyright owner can be protected.

Fifth Embodiment

Fig. 16 is a schematic block diagram to describe a structure of a cellular phone 500 according to a fifth embodiment of the present invention. Fig. 16 is comparable with Fig. 12 corresponding to the fourth embodiment.

Cellular phone 500 of the fifth embodiment shown in Fig. 16 differs in structure from cellular phone 400 of the fourth embodiment as set forth below.

Specifically, referring to Fig. 16, a memory card 150 is loaded instead

of memory card 140. When content key Kc is transmitted from memory card 150 to cellular phone 500, the content key is encrypted by session key Ks1 to be transmitted in an encrypted form of [Kc] Ks1. The double encryption with keys KPp and Ks1 in the transmission of content key Kc implemented in the previous fourth embodiment is not carried out. Therefore, the decryption process with key Ks1 can be carried out independent of the decryption process with key Kp. Cellular phone 500 shown in Fig. 16 is absent of switch 1550.

Specifically, audio reproduction module 1500 of cellular phone 500 includes a Kp hold unit 1540 to store a private decryption key Kp, a decryption processing unit 1530 to decrypt data [Ks2] Kp applied from memory card 150 via data bus BS2 using key Kp, a session key generator 1552 to generate using a random number or the like a session key Ks1 that is used to encrypt data transferred on data bus BS2 for the data transfer between memory card 150 and other components of cellular phone 500, an encryption processing unit 1554 encrypting session key Ks1 generated by session key generator 1552 with session key Ks2 from memory card 150 to provide the encrypted key onto data bus BS2, a decryption processing unit 1556 decrypting for session key Ks1 an encrypted content key Kc with session key Ks1 transmitted from memory card 150 via data bus BS2, a decryption processing unit 1520 decrypting encrypted content data [Dc] Kc applied from memory card 150 via data bus BS2 based on content key Kc output from decryption processing unit 1556 and applying the decrypted content data to audio decoding unit 1508, and a [KPp, Crtf] KPma hold unit 1560 encrypting public encryption key KPp unique to the class (type) of cellular phone 500 which is a reproduction apparatus and authentication data Crtf using public decryption key KPma common to the system to realize an authentication function with respect to cellular phone 500 for data transfer between memory card 150 and other components of cellular phone 500.

The remaining components of cellular phone 500 are similar to those of cellular phone 400 of the fourth embodiment. Corresponding components have the same reference characters allotted, and description

thereof will not be repeated.

For the sake of simplification, only the block related to distribution of content data of the present invention is depicted in Fig. 16. The block related to the conversation capability inherent to a cellular phone is partially not illustrated.

According to the structure of Fig. 16, audio decoding unit 1508, Kp hold unit 1540, decryption processing unit 1530, decryption processing unit 1520, decryption processing unit 1556, encryption processing unit 1554, session key generation unit 1552 and [KPp, Crtf] KPma hold unit 1560 can be incorporated into the TRM.

By the above structure, the authentication data, the decryption key and the data converted into plaintext cannot be modified or looked by a third party. It is therefore difficult for a third party to improperly obtain the encryption scheme and private decryption key of cellular phone 500. Thus, the security is improved.

Also, audio reproduction module 1500 corresponding to the region enclosed by a solid line in Fig. 16 can be set as the TRM. By such a structure, eventual digital data of content data subject to copyright protection subject to copyright protection such as audio data can be protected.

Structure of Memory Card

Fig. 17 is a schematic block diagram to describe a structure of memory card 150 shown in Fig. 16.

The structure of memory card 150 differs from the structure of memory card 140 of the fourth embodiment in that content key Kc is stored as plaintext data without being encrypted in memory 1412.

The remaining components of memory card 150 are similar to those of memory card 140 of the fourth embodiment. Corresponding components have the same reference characters allotted, and description thereof will not be repeated.

Memory card 150 of Fig. 17 can be incorporated into a module TRM to disable read out via a third party of data and the like in the circuitry residing in this region by erasing internal data or destroying internal

circuitry at an attempt of an improper opening process or the like by an external source.

Reproduction Process

Fig. 18 is a flow chart to describe a reproduction process of decrypting music information from encrypted content data stored in memory card 150 for music output in cellular phone 500.

Referring to the flow chart of the reproduction process of Fig. 18, application of a reproduction request (step S500) by a user's command through a keyboard 1108 or the like of cellular phone 500 causes data [KPp, Crtf] KPma to be output to memory card 150 from [KPp, Crtf] KPma hold unit 1560 of cellular phone 500 (step S502).

Decode unit 1460 of memory card 150 decrypts data [KPp, Crtf] KPma to obtain public encryption key KPp and authentication data Crtf (step S506). Controller 1420 conducts authentication of cellular phone 500 based on authentication data Crtf (step S506). When cellular phone 500 is a proper apparatus, control proceeds to step S508. When cellular phone 500 is not a proper apparatus, the operation for reproduction is not carried out, and the process ends (step S534).

When cellular phone 500 is a proper apparatus, controller 1420 causes session generator 1450 to generate a session key Ks2 (step S508). Under control of controller 1420, encryption processing unit 1452 encrypts session key Ks2 using public encryption key KPp to generate encrypted session key [Ks2] Kp. This encrypted session key [Ks2] Kp is transmitted to cellular phone 500 via data bus BS3, terminal 1202 and memory interface 1200 (step S510).

Upon reception of encrypted session key [Ks2] Kp from memory card 150 at cellular phone 500, decryption processing unit 1530 receives and decrypts encrypted session key [Ks2] Kp received via switch circuit 1550 to obtain a session key Ks2 (step S512).

At cellular phone 500, session key generation unit 1552 generates session key Ks1 (step S514). Encryption processing unit 1554 encrypts session key Ks1 using session key Ks2 extracted at step S512 to generate data [Ks1] Ks2 . Data [Ks1] Ks2 is transmitted to memory card 150 via

data bus BS2 (step S516).

Memory card 150 receives session key [Ks1] Ks2 generated and encrypted by cellular phone 500. Decryption processing unit 1454 decrypts encrypted session key [Ks1] Ks2 by session key Ks2 to extract session key Ks1 (step S518).

Then, memory card 150 reads out content key Kc from memory 1412 (step S520).

Encryption processing unit 1456 of memory card 150 encrypts content key Kc using extracted session key Ks1 to apply encrypted content key [Kc] Ks1 onto data bus BS2 via data bus BS3 and the like (step S522).

Decryption processing unit 1556 of cellular phone 500 applies a decryption process on further encrypted content key [Kc] Ks1 transmitted from memory card 150 by session key Ks1 to obtain content key Kc (step S524).

Memory card 150 reads out encrypted content key [Dc] Kc from memory 1412 and applies encrypted content data [Dc] Kc onto data bus BS2 via data bus BS3 and the like (step S530).

Decryption processing unit 1520 of cellular phone 500 decrypts encrypted content data [Dc] Kc by extracted content key Kc to generate content data Dc in plaintext. Audio decoding unit 1508 reproduces content data Dc and provides the reproduced data to combine unit 1510. Digital-analog converter 1512 converts the data received from combine unit 1510 into an analog signal to output reproduced music (step S532). Thus, the process ends (step S534).

According to the above-described structure, a reproduction operation is allowed only between memory card 150 and a cellular phone 500 verified as a proper apparatus as a result of authentication of memory card 150, based on data [KPp, Crtf] KPma from cellular phone 500. Similar to the advantages of cellular phone 400 and memory card 130 of the previous fourth embodiment, protection on the copyright of the copyright owner can be conducted with a more simple structure.

Sixth Embodiment

Fig. 19 is a schematic block diagram to describe a structure of a

cellular phone 600 according to a sixth embodiment of the present invention. Fig. 19 is comparable with Fig. 16 corresponding to the fifth embodiment.

Cellular phone 600 of the sixth embodiment shown in Fig. 19 differs in structure from cellular phone 500 of the fifth embodiment as set forth below.

Referring to Fig. 19, cellular phone 600 includes a Kcom hold unit 1570 to store a private decryption key Kcom common to the system, and a decryption processing unit 1572 decrypting the output from decryption processing unit 1556 using private decryption key Kcom to obtain content key Kc, which is supplied to decryption processing unit 1520.

In contrast to the previous fifth embodiment where content key Kc is transmitted from memory card 150 to cellular phone 500 in the form of content key [Kc] Ks1 encrypted using session key Ks1, the sixth embodiment has the transmitted content key Kc from memory card 160 to cellular phone 600 in the form of encrypted content key [[Kc] Kcom] Ks1 that can be decrypted using private decryption key Kcom and session key Ks1.

The remaining components of cellular phone 600 are similar to those of cellular phone 500 of the fifth embodiment. Corresponding components have the same reference characters allotted, and description thereof will not be repeated.

For the sake of simplification, only the block related to distribution of audio data in the present invention is depicted in Fig. 19. The block related to the conversation function inherent to a cellular phone is partially not illustrated.

According to the structure shown in Fig. 19, audio decoding unit 1508, Kp hold unit 1540, decryption processing unit 1530, decryption processing unit 1520, decryption processing unit 1556, encryption processing unit 1554, session key generation unit 1552, [KPp, Crtf] KPma hold unit 1560, Kcom hold unit 1570 and decryption processing unit 1572 can be incorporated into a TRM.

By such a structure, a third party cannot obtain the authentication

data, decryption key and content data in a plaintext form improperly. Therefore, the security is improved.

Also, audio reproduction module 1500 corresponding to the region enclosed by a solid line in Fig. 19 can be set as the TRM. By such a structure, eventual digital data of data subject to copyright protection such as audio data can be protected.

Structure of Encryption/Decryption Key

Fig. 20 is a diagram to describe together characteristics of key data for communication used in cellular phone 600 shown in Fig. 19.

According to the structure of Fig. 19, the key to control data processing in memory card 160 includes a public decryption key KPma common to the system, and a session key Ks2 unique to each section, and generated by memory card 160.

The encryption key to maintain security during data transfer with an external source to the memory card includes a public encryption key KPp unique to the class of the reproduction apparatus which is a cellular phone here, stored in [KPp, Crtf] KPma hold unit 1560 of cellular phone 600 in an encrypted form with key KPma as a key to control audio reproduction module 1500, a private decryption key Kp asymmetric to key KPp, and used to decrypt data encrypted with key KPp, a private decryption key Kcom common to the system, and a session key Ks1 which is a symmetric key generated by session key generator 1552 for each session.

Session key Ks1 has a value unique to each communication session, and is under control in audio reproduction module 1500.

With regards to copyright data recorded in memory card 160, it is assumed that encrypted content data is decrypted (converted into plaintext) using a symmetric key Kc that is a symmetric key directed to encrypt audio data (content data) per se.

When content key Kc is distributed from distribution server 10 towards cellular phone 600, it is assumed that content key Kc is at least encrypted so as to be decryptable by private decryption key Kcom, and stored in memory card 160 as encrypted content data [Kc] Kcom.

Also, it is assumed that content data Dc subject to copyright

protection is stored in memory card 160 as encrypted content data [Dc] Kc that can be decrypted using content key Kc.

Structure of Memory Card

Fig. 21 is a schematic block diagram to describe a structure of memory card 160 shown in Fig. 19.

Memory card 160 differs in structure from memory card 150 of the fifth embodiment in that content data Kc is stored in memory 1412 as encrypted data [Kc] Kcom.

The remaining components of memory card 160 are similar to those of memory card 150 of the fifth embodiment. Corresponding components have the same reference characters allotted, and the description thereof will not be repeated.

Memory card 160 of Fig. 21 can be incorporated into a module TRM to disable read out by a third party of data and the like in the circuitry residing in this region by erasing internal data or destroying internal circuitry at an attempt of an improper opening process or the like by an external source.

Reproduction Process

Fig. 22 is a flow chart to describe a reproduction process of reproducing music from encrypted content data stored in memory card 160 for output.

Referring to Fig. 22, upon application of a reproduction request by a user's command through keyboard 108 or the like of cellular phone 600 (step S600), data [KPp, Crtf] KPma is output to memory card 160 from [KPp, Crtf] KPma hold unit 1560 of cellular phone 600 (step S602).

Decode unit 1460 of memory card 160 decrypts data [KPp, Crtf] KPma to obtain public encryption key KPp and authentication data Crtf (step S606). Controller 1420 conducts authentication of cellular phone 600 based on authentication data Crtf (step S606). When cellular phone 600 is a proper apparatus, control proceeds to step S608. When cellular phone 600 is not a proper apparatus, the process ends without carrying out an operation for reproduction (step S634).

When cellular phone 600 is a proper apparatus, controller 1420

causes session key generator 1450 to generate a session key Ks2 (step S608). Under control of controller 1420, encryption processing unit 1452 encrypts public encryption key KPp using session key Ks2 to generate encrypted session key [Ks2] Kp. This encrypted session key [Ks2] Kp is transmitted to cellular phone 600 via data bus BS3, terminal 1202 and memory interface 1200 (step S610).

Upon reception of encrypted section key [Ks2] Kp from memory card 160 at cellular phone 600, decryption processing unit 1530 decrypts encrypted session key [Ks2] Kp received from decryption processing unit 1530 to obtain session key Ks2 (step S612).

Session key generation unit 1552 of cellular phone 600 generates session key Ks1 (step S614). Encryption processing unit 1554 encrypts session key Ks1 using session key Ks2 extracted at step S612 to generate encrypted session key [Ks1] Ks2. Encrypted session key [Ks1] Ks2 is transmitted to card 160 via data bus BS2 (step S616).

Memory card 160 receives encrypted session key [Ks1] Ks2 generated by cellular phone 600. Decryption processing unit 1454 decrypts the received encrypted session key [Ks1] Ks2 by session key Ks2 to extract session key Ks1 (step S618).

Then, memory card 160 reads out encrypted content key [Kc] Kcom from memory 1412 (step S620).

Then, encryption processing unit 1456 of memory card 160 encrypts encrypted content key [Kc] Kcom using extracted content key Ks1 to apply the further encrypted content key [[Kc] Kcom] Ks1 onto data bus BS2 via data bus BS3 and the like (step S622).

Decryption processing unit 1556 of cellular phone 600 decrypts further encrypted content key [[Kc] Kcom] Ks1 transmitted from memory card 160 by session key Ks1 to obtain encrypted content key [Kc] Kcom (step S624).

Decryption processing unit 1572 of cellular phone 600 receives encrypted content key [Kc] Kcom from decryption processing unit 1556 to apply a decryption process on encrypted content key [Kc] Kcom based on key Kcom from Kcom hold unit 1570 (step S626).

When content key Kc can be extracted by a decryption process by decryption processing unit 1572 (step S628), control proceeds to step S630, otherwise (step S628), the process ends (step S634).

When a content key Kc is extracted by the decryption process of decryption processing unit 1572, memory card 160 reads out encrypted content data [Dc] Kc from memory 1412 and applies the same to data bus BS2 via data bus BS3 and the like (step S630).

Decryption processing unit 1520 of cellular phone 600 decrypts encrypted content data [Dc] Kc using extracted content key Kc to generate content data Dc in plaintext. Audio decoding unit 1508 reproduces content data Dc and applies the reproduced content data to combine unit 1510. Digital-analog converter 1512 converts the data received from combine unit 1510 to output the reproduced music (step S632). Thus, the process ends (step S634).

According to the above-described structure, a reproduction operation is allowed only between memory card 160 and a cellular phone 600 verified as a proper apparatus as a result of authentication by memory card 160, based on data [KPp, Crtf] KPma from cellular phone 600. Therefore, similar to the advantages provided by cellular phone 400 and memory card 140 of the fourth embodiment, the security of the system can be improved and the copyright of the copyright owner can be prevented.

Although the present invention has been described and illustrated in detail, it is clearly understood that the same is by way of illustration and example only and is not to be taken by way of limitation, the spirit and scope of the present invention being limited only by the terms of the appended claims.

CLAIMS

1. A data recording apparatus (100) decrypting encrypted content data to reproduce content data, comprising:

a data storage unit (110, 120, 130) to store said encrypted content data and an encrypted content key which is an encrypted version of a content key directed to decrypt said encrypted content data, and

a data reproduction unit (1500) receiving an output from said data storage unit to reproduce said encrypted content data,

wherein said data reproduction unit comprises

a first key hold unit (1540) storing a first decryption key used to decrypt said encrypted content key read out from said data storage unit,

a first decryption processing unit (1530) extracting said content key by applying a decryption process by an output from said first key hold unit based on said encrypted content key from said data storage unit, and

a second decryption processing unit (1520) receiving said encrypted content data read out from said data storage unit, and applying a decryption process by an output of said first decryption processing unit to extract content data.

2. The data reproduction apparatus according to claim 1, wherein said data reproduction unit further comprises

a first session key generation unit (1502) generating a first session key updated at every time of access to obtain said encrypted content data for said data storage unit,

a first encryption processing unit (1504) encrypting said first session key with a first encryption key that is decryptable at said data storage unit and applying the encrypted first session key to said data storage unit, and

a third decryption processing unit (1506) decrypting for said first session key said encrypted content key obtained from said data storage unit in a further encrypted form with said first session key, and providing the decrypted encrypted content key to said first decryption processing unit.

3. The data reproduction apparatus according to claim 2, said content data being coded audio data coded according to a coding scheme to reduce an amount of data,

wherein said data reproduction unit comprises

an audio decoding unit (1508) reproducing audio data based on said coding scheme from said coded audio data, and

a digital-analog converter (1512) converting said reproduced audio data into an analog signal.

4. The data reproduction apparatus according to claim 3, wherein said data reproduction unit is provided in a security region that cannot be read out by a third party.

5. The data reproduction apparatus according to claim 2, wherein said data storage unit (120) includes

a memory unit (1412) to store data applied to said data storage unit,

a second key hold unit (1401) storing said first encryption key,

a third key hold unit (1402) to store a second decryption key directed to decrypt data encrypted with said first encryption key,

a fourth decryption processing unit (1404) to decrypt said first session key transmitted from said data reproduction unit in an encrypted form by said first encryption key based on said second decryption key, and

a second encryption processing unit (1406) encrypting data stored in said memory unit using said first session key extracted by said fourth decryption processing unit for output.

6. The data reproduction apparatus according to claim 5, wherein said data storage unit is a memory card detachable with respect to said data reproduction unit.

7. The data reproduction apparatus according to claim 1, said data reproduction unit receiving supply of a second session key differing for each access to obtain said encrypted content data with respect to said data

storage unit, and encrypted to be decryptable by said first decryption key,

wherein said data reproduction unit comprises

a first session key generation unit (1552) generating a first session key updated for each access to obtain said encrypted content data with respect to said data storage unit,

a second encryption processing unit (1554) encrypting said first session key using said second session key extracted by said first decryption processing unit based on said first decryption key from externally applied data, and applying the encrypted first session key to said data storage unit, and

a third decryption processing unit (1556) decrypting for said first session key said encrypted content key obtained from said data storage unit in a further encrypted form with said first session key, and providing the decrypted encrypted content key to said first decryption processing unit.

8. The data reproduction apparatus according to claim 7, said content data being coded audio data coded by a coding scheme to reduce an amount of data,

wherein said data reproduction unit comprises

an audio decoding unit reproducing audio data based on said coding method from said coded audio data, and

a digital-analog converter converting said reproduced audio data into an analog signal.

9. The data reproduction apparatus according to claim 8, wherein said data reproduction unit is provided in a security region that cannot be read out by a third party.

10. The data reproduction apparatus according to claim 7, wherein said data storage unit (130) comprises

a memory unit (1412) to store data applied to said data storage unit,

a second session key generation unit (1450) generating a second session key updated for every access to obtain said encrypted content data,

a third encryption processing unit (1452) carrying out an encryption process by a second encryption key that is decryptable with said first decryption key,

a fifth decryption processing unit (1454) to decrypt said first session key transmitted from said data reproduction unit in an encrypted form with said second session key, based on said second session key, and

a fourth encryption processing unit (1456) encrypting data stored in said memory unit using said first session key extracted by said fifth decryption processing means for output.

11. The data reproduction apparatus according to claim 10, wherein said data storage unit is a memory card detachable with respect to said data reproduction unit.

12. The data reproduction apparatus according to claim 1, wherein said data reproduction unit has at least said first key hold unit, said first decryption processing unit and said second decryption processing unit provided in a security region that cannot be read out by a third party.

13. A data reproduction apparatus decrypting encrypted content data to reproduce content data, comprising:

a data storage unit (140, 150, 160) storing said encrypted content data and a content key directed to decrypt said encrypted content data, and detachable with respect to said data reproduction apparatus, and

a data reproduction unit (1500) receiving an output from said data storage unit to reproduce said encrypted content data,

wherein said data reproduction unit comprises

a first decryption processing unit (1520) receiving and decrypting said encrypted content data read out from said data storage unit to extract content data, and

an authentication data hold unit (1560) storing authentication data in an encrypted form that is decryptable by an authentication key, and that can output the encrypted authentication data to said data storage unit,

wherein said data storage unit comprises

a second decryption processing unit (1460) decrypting said authentication data applied from said data reproduction unit in an encrypted form with said authentication key to extract the decrypted authentication data, and

control means (1420) for carrying out an authentication process based on said authentication data extracted by said second decryption processing unit.

14. The data reproduction apparatus according to claim 13, wherein said data reproduction unit further comprises

a session key generation unit (1552) generating a first session key that is updated at every time of access to obtain said encrypted content key with respect to said data storage unit,

an encryption processing unit (1554) encrypting said session key with a first encryption key that is decryptable by said data storage unit to apply the encrypted session key to said data storage unit (1554), and

a third decryption processing unit (1556) decrypting for said first session key said encrypted content key received from said data storage unit in an encrypted form with said first session key.

15. The data reproduction apparatus according to claim 14, wherein said third decryption processing unit applies a decrypted result to said first decryption processing unit as a content key directed to decrypt said encrypted content data.

16. The data reproduction apparatus according to claim 14, wherein said authentication data hold unit encrypts a second encryption key directed to apply encryption that is decryptable with a first decryption key as well as said authentication data into a form decryptable with said authentication key for output to said data storage unit,

wherein said data reproduction unit further comprises a fourth decryption processing unit (1530) decrypting by said first decryption key

said first encryption key received from said data storage unit in an encrypted form with said second encryption key, and applying the decrypted first encryption key to said encryption processing unit.

17. The data reproduction apparatus according to claim 16, wherein said fourth decryption processing unit (1530) receives said content key from said data storage unit in a form encrypted with said second encryption key so as to be decryptable with said first decryption key and further encrypted with said first session key as a decrypted result of said first session key by said third decryption processing unit, and decrypting the content key encrypted for said second encryption key using said first decryption key to apply the decrypted content key to said first decryption processing unit.

18. The data reproduction apparatus according to claim 14, wherein said data reproduction unit further comprises a fifth decryption processing unit (1572) to apply decryption with a predetermined second decryption key,

said fifth decryption processing unit receiving said content key from said data storage unit in an encrypted form decryptable with said second decryption key and further encrypted with said first session key as a decrypted result for said first session key by said third decryption unit, and applying decryption with said second decryption key to provide the decrypted content key to said first decryption processing unit.

19. The data reproduction apparatus according to claim 13, wherein said data storage unit is a memory card detachable with respect to said data reproduction unit.

20. The data reproduction apparatus according to claim 13, wherein said data reproduction apparatus further comprises an interface to connect with a cellular phone network including a simple portable telephone network.

21. The data reproduction apparatus according to claim 20, further

comprising a conversation processing unit to effect conversation via said interface.

22. The data reproduction apparatus according to claim 21, wherein said data storage unit is detachable with respect to said data reproduction unit.

ABSTRACT

A cellular phone (100) has distributed encrypted content data and an encrypted content key stored in a memory (110). The encrypted content key data read out from the memory (110) is decrypted by a decryption processing unit (1530) using key data Kp stored in a Kp hold unit (1540), and then applied to a audio reproduction module (1500). A decryption processing unit (1520) decrypts encrypted content data read out from the memory (110) using a content key Kc extracted by the decryption processing unit (1530) to reproduce content data Dc.

FIG.1

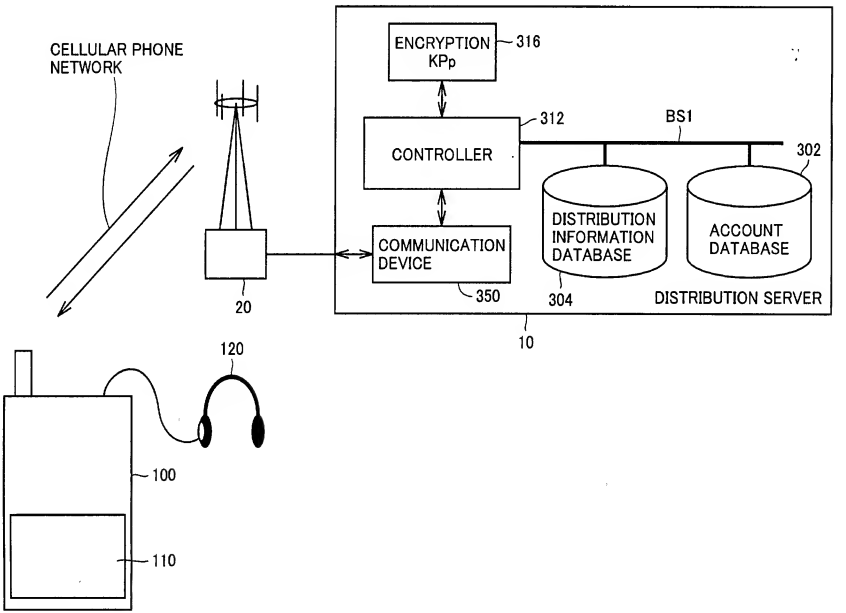


FIG.2

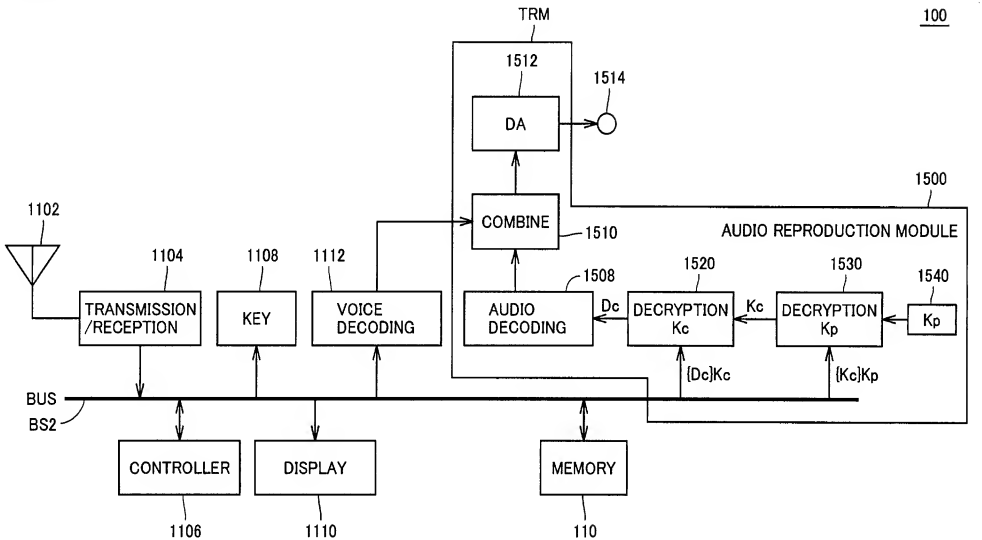


FIG.3

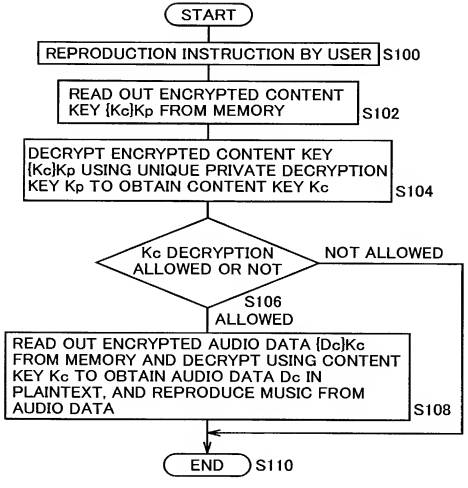

START
REPRODUCTION INSTRUCTION BY USER
S100
READ OUT ENCRYPTED CONTENT KEY {Kc}Kp FROM MEMORY
S102
DECRYPT ENCRYPTED CONTENT KEY {Kc}Kp USING UNIQUE PRIVATE DECRYPTION KEY Kp TO OBTAIN CONTENT KEY Kc
S104
Kc DECRYPTION ALLOWED OR NOT
NOT ALLOWED
S106
ALLOWED
READ OUT ENCRYPTED AUDIO DATA {Dc}Kc FROM MEMORY AND DECRYPT USING CONTENT KEY Kc TO OBTAIN AUDIO DATA Dc IN PLAINTEXT, AND REPRODUCE MUSIC FROM AUDIO DATA
S108
END
S110

FIG.4

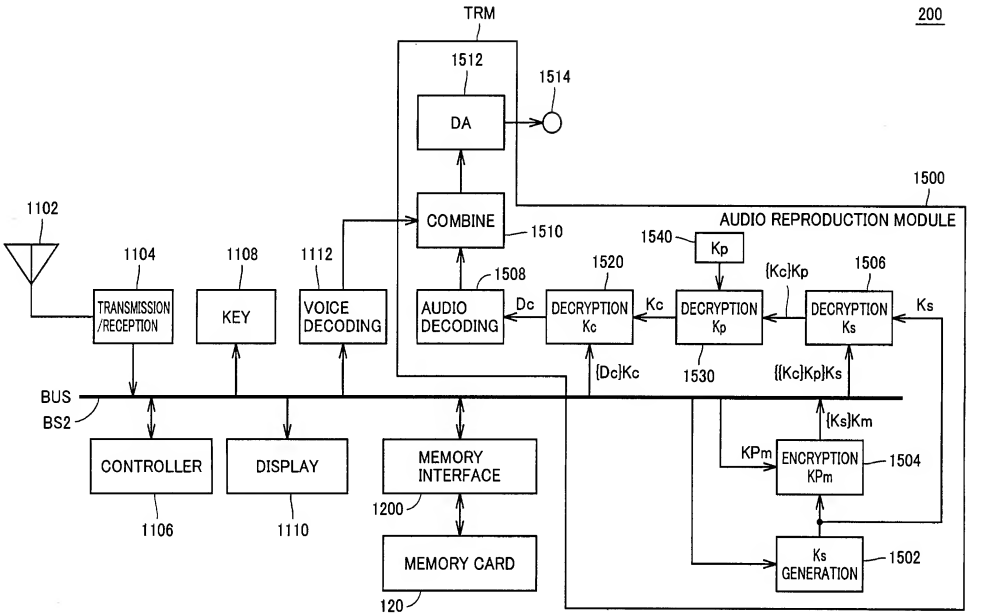


FIG.5

	SYMBOL	ATTRIBUTE	PROPERTY	
KEY ADMINISTERED WITHIN MEMORY CARD	Km	PRIVATE DECRYPTION KEY		UNIQUE TO EACH MEMORY CARD
	KPm	PUBLIC ENCRYPTION KEY	FORM PAIR WITH Km	DATA ENCRYPTED WITH KPm IS DECRYPTABLE WITH ASYMMETRIC DECRYPTION KEY Km
KEY ADMINISTERED IN AUDIO REPRODUCTION MODULE	Kp	PRIVATE DECRYPTION KEY	UNIQUE TO DATA REPRODUCTION APPARATUS (CELLULAR PHONE)	DIFFER FOR EACH DATA REPRODUCTION APPARATUS
	Ks	SYMMETRIC KEY	UNIQUE TO SESSION	GENERATED FOR EVERY ACCESS BETWEEN MEMORY AND AUDIO REPRODUCTION MODULE
DISTRIBUTION DATA	KPp	PUBLIC ENCRYPTION KEY	FORM PAIR WITH Kp (ENCRYPT Kc)	DATA ENCRYPTED WITH KPp CAN BE DECRYPTED USING ASYMMETRIC DECRYPTION KEY Kp
	Kc	SYMMETRIC KEY	CONTENT KEY	DECRYPTION KEY OF ENCRYPTED CONTENT DATA
	Dc	CONTENT DATA		EXAMPLE: AUDIO DATA

FIG.6

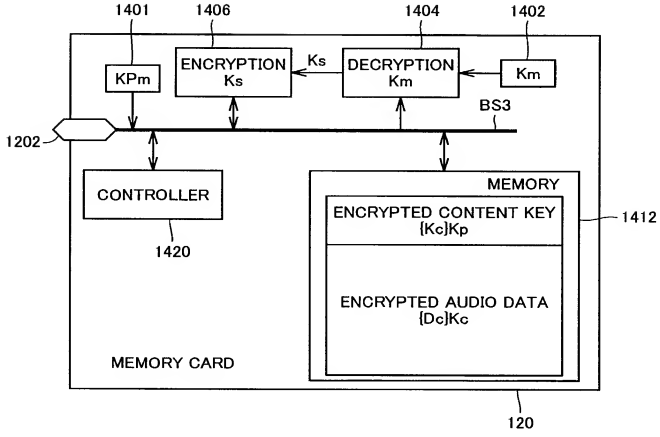

1401
1406
1404
1402
KPm
ENCRYPTION Ks
Ks
DECRYPTION Km
Km
BS3
1202
CONTROLLER
1420
MEMORY
ENCRYPTED CONTENT KEY {Kc}Kp
1412
ENCRYPTED AUDIO DATA {Dc}Kc
MEMORY CARD
120

FIG.7

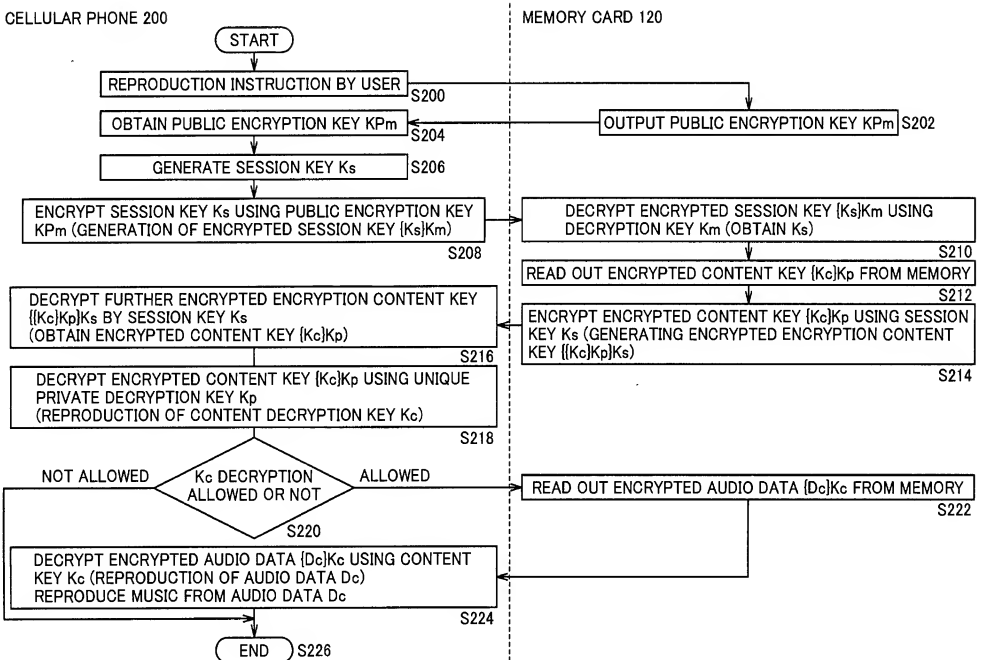


FIG.8

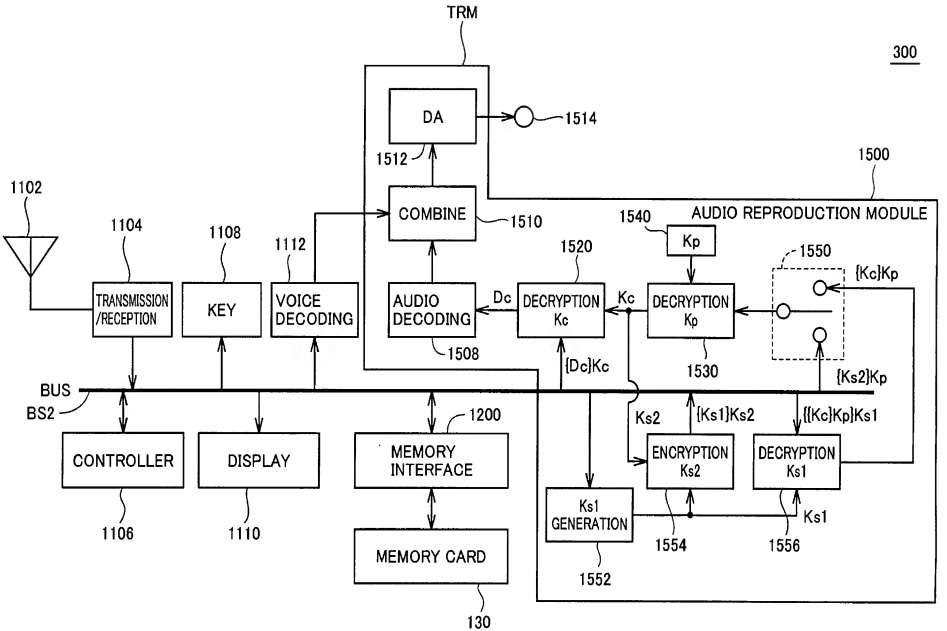


FIG.9

	SYMBOL	ATTRIBUTE	PROPERTY	
KEY ADMINISTERED WITHIN MEMORY CARD	Km	PRIVATE DECRYPTION KEY		UNIQUE TO EACH MEMORY CARD
	KPm	PUBLIC ENCRYPTION KEY		DATA ENCRYPTED WITH KPm IS DECRYPTABLE WITH ASYMMETRIC DECRYPTION KEY Km
	Ks2	SYMMETRIC KEY	UNIQUE TO SESSION	GENERATED FOR EVERY ACCESS BETWEEN MEMORY AND AUDIO REPRODUCTION MODULE
KEY ADMINISTERED IN AUDIO REPRODUCTION MODULE	Kp	PRIVATE DECRYPTION KEY	UNIQUE TO DATA REPRODUCTION APPARATUS (CELLULAR PHONE)	DIFFER FOR EACH DATA REPRODUCTION APPARATUS
	Ks1	SYMMETRIC KEY	UNIQUE TO SESSION	GENERATED FOR EVERY ACCESS BETWEEN MEMORY AND AUDIO REPRODUCTION MODULE
DISTRIBUTION DATA	KPp	PUBLIC ENCRYPTION KEY		DATA ENCRYPTED WITH KPp CAN BE DECRYPTED USING ASYMMETRIC DECRYPTION KEY Kp
	Kc	SYMMETRIC KEY	CONTENT KEY	DECRYPTION KEY OF ENCRYPTED CONTENT DATA
	Dc	CONTENT DATA		EXAMPLE: AUDIO DATA

FIG.10

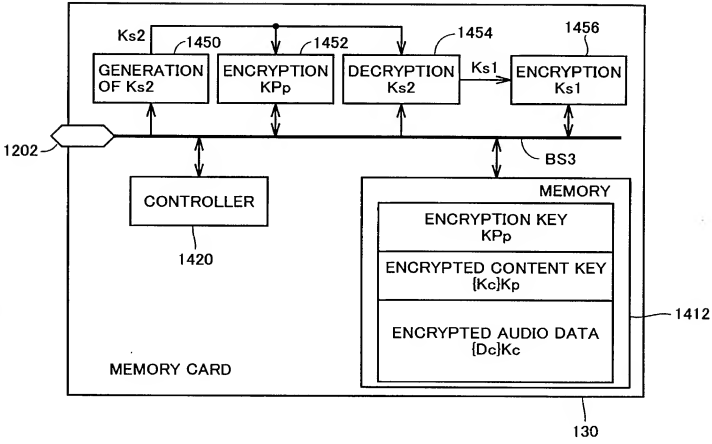

Ks2
1450
1452
1454
1456
GENERATION OF Ks2
ENCRYPTION KPp
DECRYPTION Ks2
Ks1
ENCRYPTION Ks1
1202
BS3
CONTROLLER
1420
MEMORY
ENCRYPTION KEY KPp
ENCRYPTED CONTENT KEY [Kc]Kp
ENCRYPTED AUDIO DATA [Dc]Kc
1412
MEMORY CARD
130

FIG.11

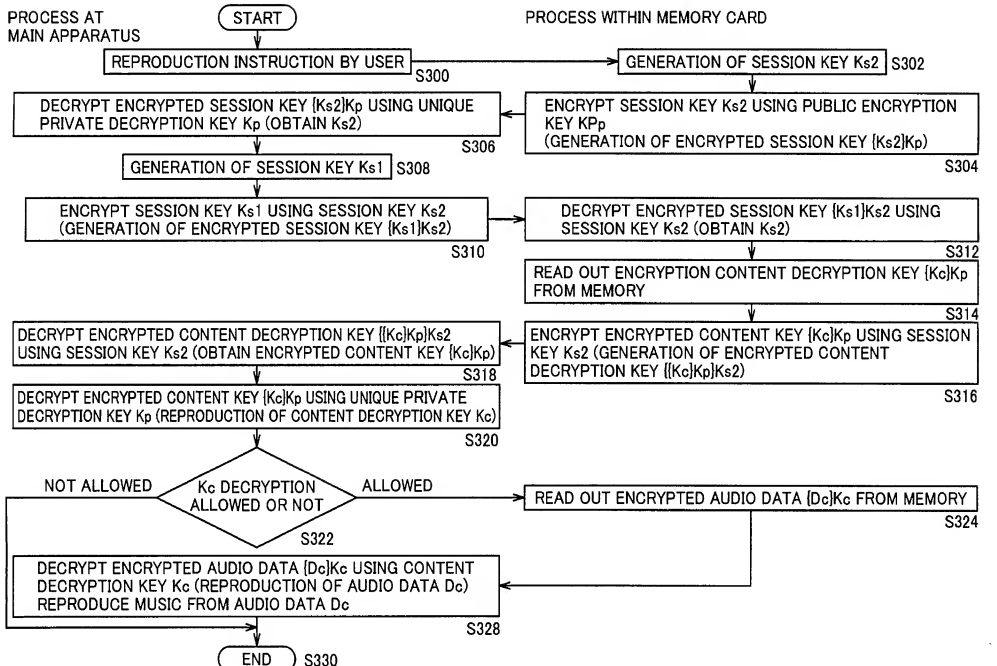


FIG.12

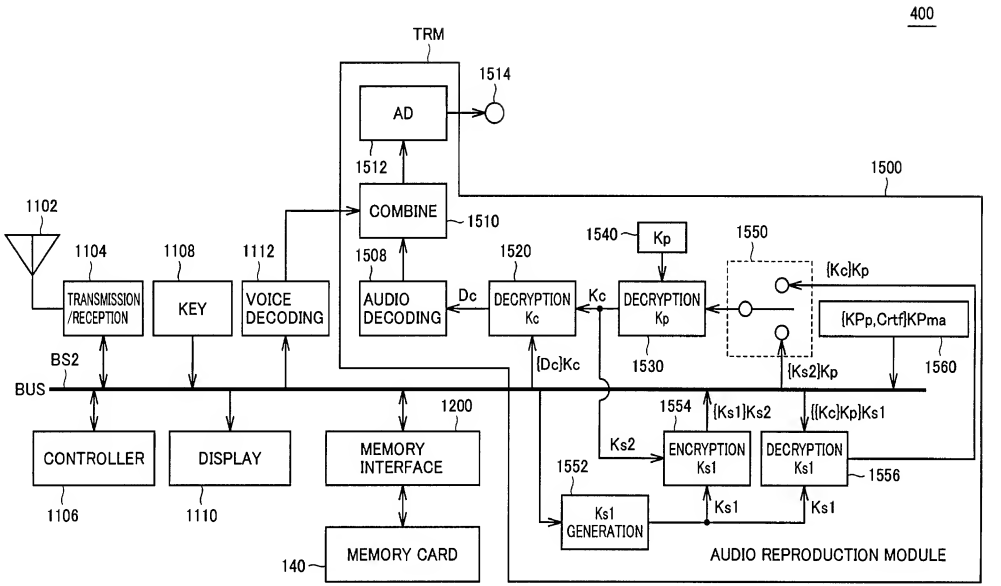


FIG. 13

	SYMBOL	ATTRIBUTE	PROPERTY	
KEY ADMINISTERED WITHIN MEMORY CARD	KPma	PUBLIC DECRYPTION KEY	COMMON TO SYSTEM	AUTHENTICATION KEY HAVING CAPABILITY TO VERIFY AUTHENTICATION OF KPp BY DECRYPTION OF {KPp, Crtf} KPma
	Ks2	SYMMETRIC KEY	SESSION KEY	GENERATED FOR EVERY ACCESS BETWEEN MEMORY AND AUDIO REPRODUCTION MODULE
KEY ADMINISTERED IN AUDIO REPRODUCTION MODULE	KPp	PUBLIC ENCRYPTION KEY	UNIQUE TO CLASS (TYPE) OF REPRODUCTION APPARATUS	DECRYPTABLE USING ASYMMETRIC PRIVATE DECRYPTION KEY Kp DIFFERING FOR EACH DATA REPRODUCTION APPARATUS OR TYPE OF REPRODUCTION DATA APPARATUS
	Kp	PRIVATE DECRYPTION KEY	UNIQUE TO CLASS (TYPE) OF REPRODUCTION APPARATUS	CONVERT INTO PLAINTEXT ENCRYPTED DATE ENCRYPTED USING ASYMMETRIC PRIVATE DECRYPTION KEY Kp DIFFERING FOR EACH DATA REPRODUCTION APPARATUS OR TYPE OF REPRODUCTION DATA APPARATUS
	Ks1	SYMMETRIC KEY	UNIQUE TO SESSION	GENERATED FOR EVERY ACCESS BETWEEN MEMORY CARD AND AUDIO REPRODUCTION MODULE
DISTRIBUTION DATA	Kc	SYMMETRIC KEY	CONTENT KEY	DECRYPTION KEY OF ENCRYPTED CONTENT DATA
	Dc	DATA	CONTENT DATA	EXAMPLE: AUDIO DATA

FIG.14

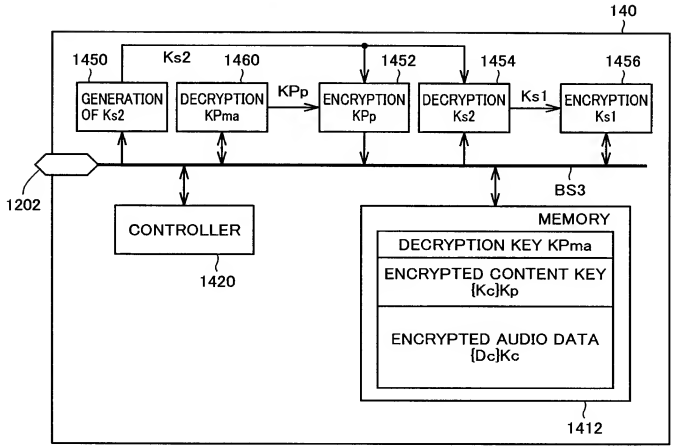

140
1450
Ks2
1460
1452
1454
1456
GENERATION OF Ks2
DECRYPTION KPma
KPp
ENCRYPTION KPp
DECRYPTION Ks2
Ks1
ENCRYPTION Ks1
1202
BS3
CONTROLLER
1420
MEMORY
DECRYPTION KEY KPma
ENCRYPTED CONTENT KEY {Kc}Kp
ENCRYPTED AUDIO DATA {Dc}Kc
1412

FIG.15

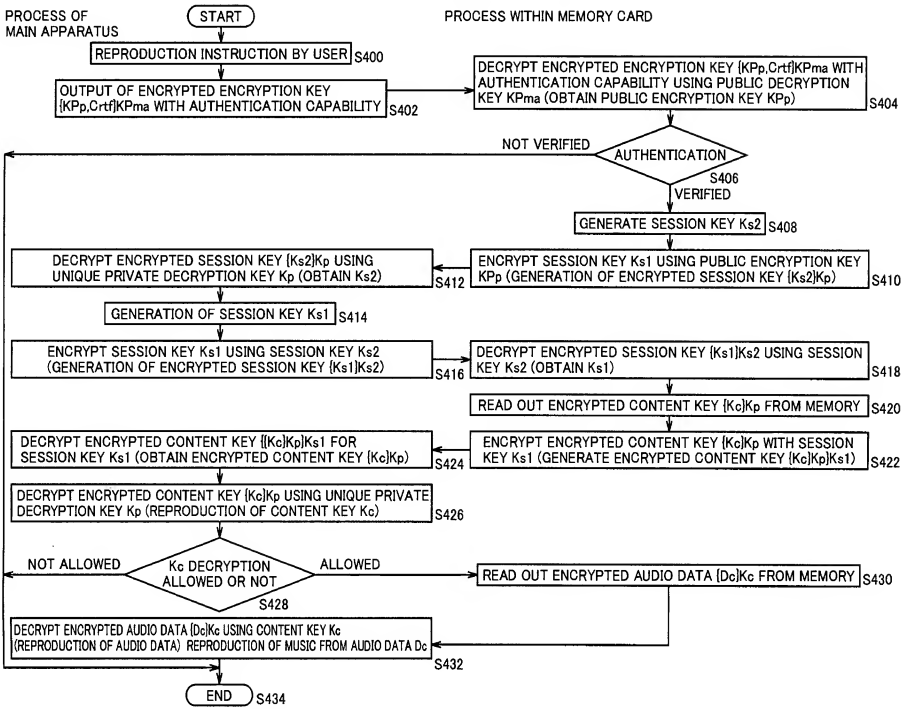


FIG.16

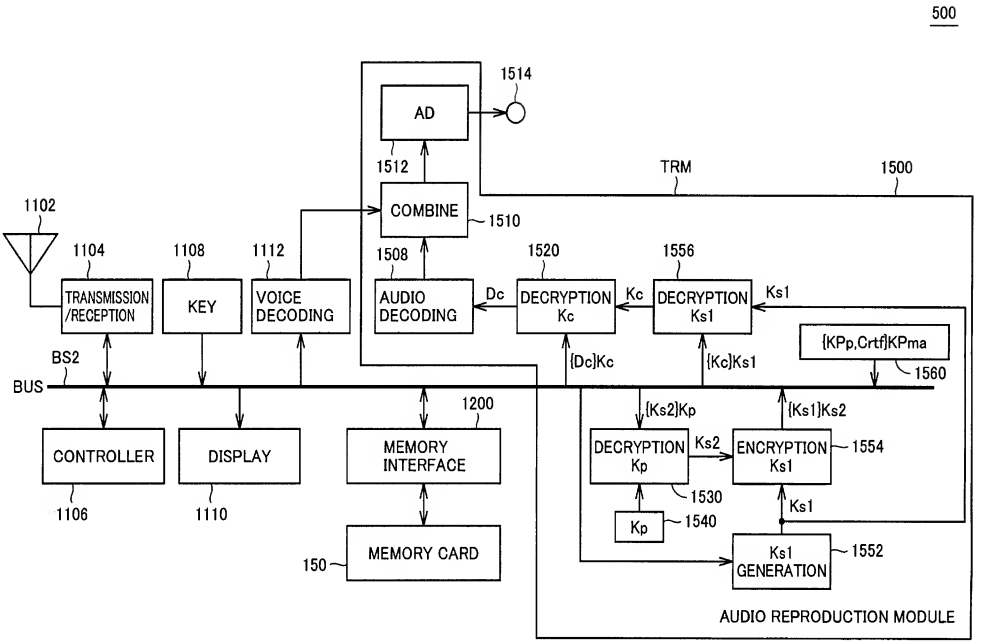


FIG.17

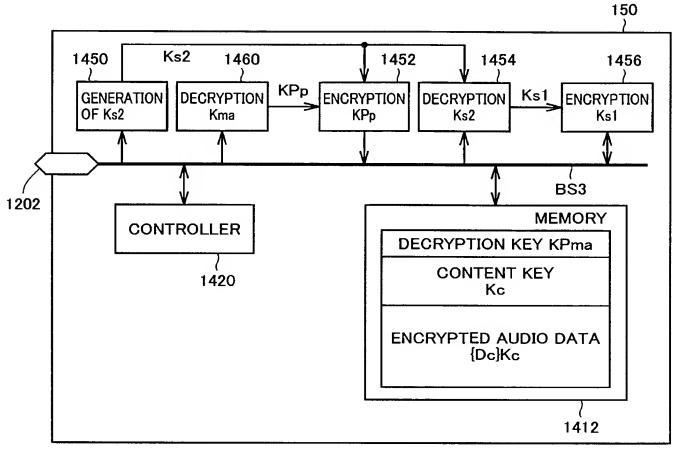

150
1450
Ks2
1460
1452
1454
1456
GENERATION OF Ks2
DECRYPTION Kma
KPp
ENCRYPTION KPp
DECRYPTION Ks2
Ks1
ENCRYPTION Ks1
1202
BS3
CONTROLLER
1420
MEMORY
DECRYPTION KEY KPma
CONTENT KEY Kc
ENCRYPTED AUDIO DATA {Dc}Kc
1412

FIG.18

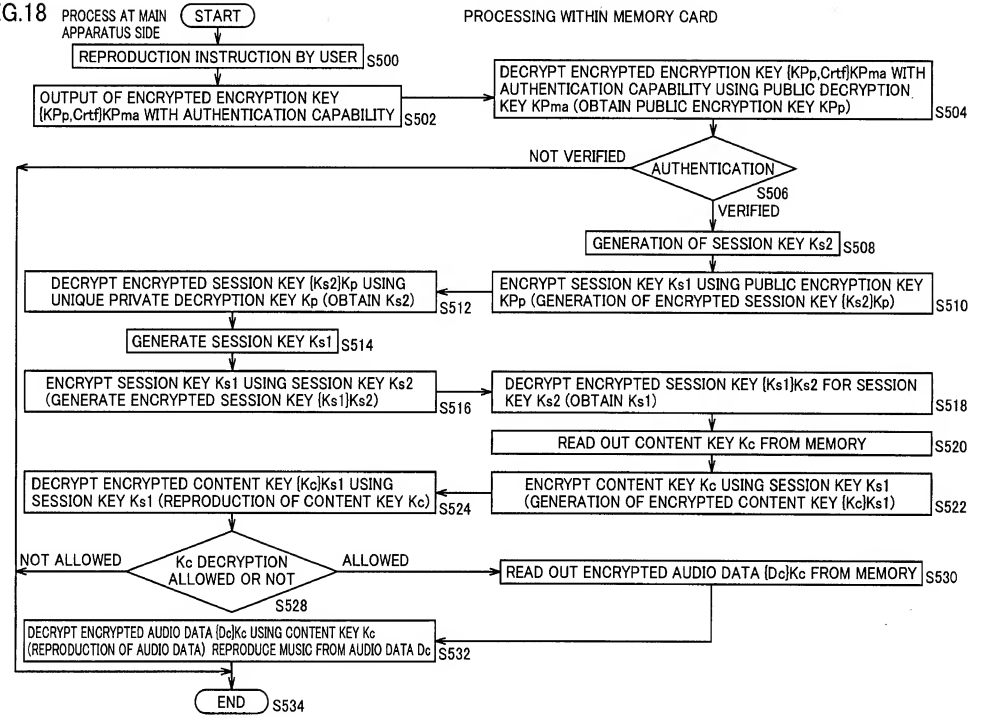


FIG.19

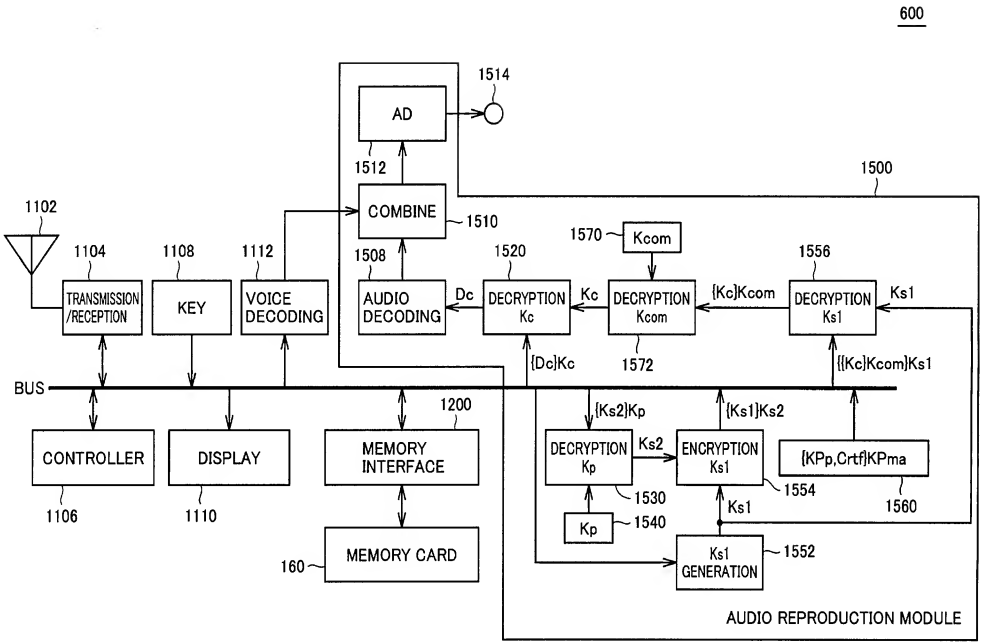


FIG. 20

	SYMBOL	ATTRIBUTE	PROPERTY	
KEY ADMINISTERED WITHIN MEMORY CARD	KPma	PUBLIC DECRYPTION KEY	COMMON TO SYSTEM	AUTHENTICATION KEY HAVING CAPABILITY TO VERIFY AUTHENTICATION OF KPp BY DECRYPTION OF {KPp, Crtf} KPma
	Ks2	SYMMETRIC KEY	SESSION KEY	GENERATED FOR EVERY ACCESS BETWEEN MEMORY AND AUDIO REPRODUCTION MODULE
KEY ADMINISTERED IN AUDIO REPRODUCTION MODULE	KPp	PUBLIC ENCRYPTION KEY	UNIQUE TO CLASS (TYPE) OF REPRODUCTION APPARATUS	DECRYPTABLE USING ASYMMETRIC PRIVATE DECRYPTION KEY Kp DIFFERING FOR EACH DATA REPRODUCTION APPARATUS OR TYPE OF REPRODUCTION DATA APPARATUS
	Kp	PRIVATE DECRYPTION KEY	UNIQUE TO CLASS (TYPE) OF REPRODUCTION APPARATUS	CONVERT INTO PLAINTEXT ENCRYPTED DATE ENCRYPTED USING ASYMMETRIC PRIVATE DECRYPTION KEY Kp DIFFERING FOR EACH DATA REPRODUCTION APPARATUS OR TYPE OF REPRODUCTION DATA APPARATUS
	Kcom	PRIVATE DECRYPTION KEY	COMMON TO SYSTEM	DECRYPT ENCRYPTED CONTENT KEY
	Ks1	SYMMETRIC KEY	UNIQUE TO SESSION	GENERATED FOR EVERY ACCESS BETWEEN MEMORY AND AUDIO REPRODUCTION MODULE
DISTRIBUTION DATA	Kc	SYMMETRIC KEY	CONTENT KEY	DECRYPTION KEY OF ENCRYPTED CONTENT DATA
	Dc	DATA	CONTENT DATA	EXAMPLE: AUDIO DATA

FIG.21

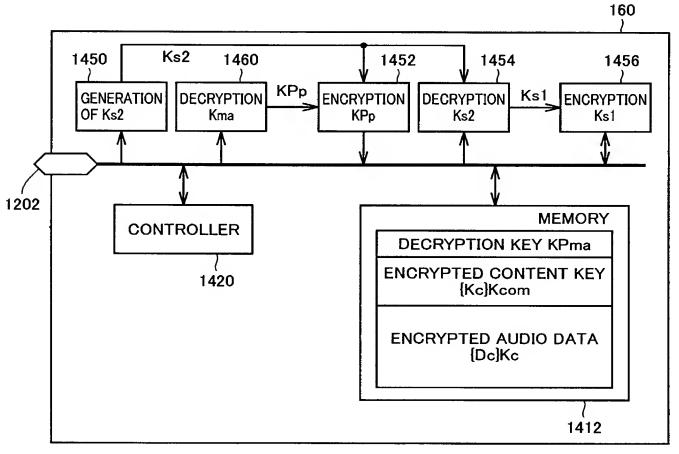
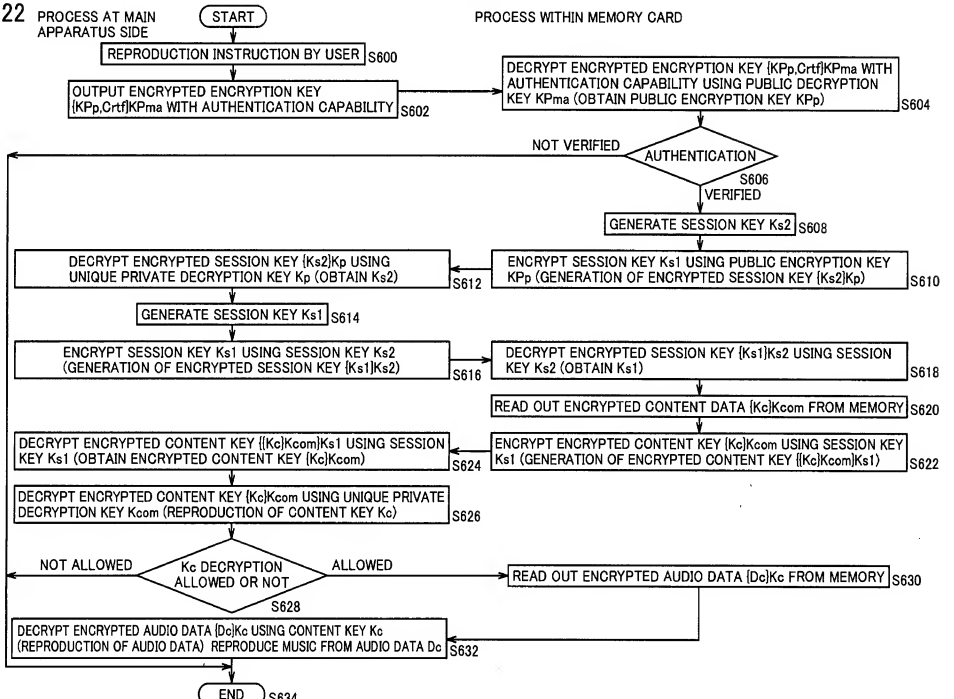

160
1450
Ks2
1460
1452
1454
1456
GENERATION OF Ks2
DECRYPTION Kma
KPp
ENCRYPTION KPp
DECRYPTION Ks2
Ks1
ENCRYPTION Ks1
1202
CONTROLLER
1420
MEMORY
DECRYPTION KEY KPma
ENCRYPTED CONTENT KEY {Kc}Kcom
ENCRYPTED AUDIO DATA {Dc}Kc
1412

FIG.22



Docket No. P806-698-A020234

Armstrong, Westerman & Hattori, LLP

DECLARATION FOR U.S. PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Data Reproduction Apparatus and Data Reproduction Module

the specification of which is attached hereto unless the following is checked

☒ was filed on August 29, 2000 as PCT International Application Number PCT/JP00/05832 and was amended on June 20, 2001 (if applicable).

☒ was filed on February 28, 2002 as United States Application Number 10/069,118 and was amended on February 28, 2002 (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 (a) - (d) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application for which priority is claimed.

	(Number)	(Country)	(Day/Month/Year Filed)	Priority Claimed
(List prior foreign applications. See note A)	11-243583 Pat.	Japan	30/August/1999	x Yes __ No
	11-343707 Pat.	Japan	02/December/1999	x Yes __ No
				__ Yes __ No
				__ Yes __ No

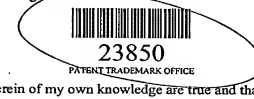
(See note B) __ See attached list for additional prior foreign applications

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

	(Application Serial No.)	(Filing Date)	Status
(List prior U.S. Applications)			__ Patented __ Pending __ Abandoned
			__ Patented __ Pending __ Abandoned
			__ Patented __ Pending __ Abandoned
			__ Patented __ Pending __ Abandoned

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Please direct all communications to the following address:



I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18 of the United States Code, § 1001 and that such willful false statements my jeopardize the validity of the application or any patent issued thereon.

1-00

(See note C) Full name of sole or first inventor (given name, family name) Masayuki HATANAKA

Inventor's Signature Masayuki Hatanaka Date May 17, 2002

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

2-00

Full name of second inventor (given name, family name) Jun KAMADA

Inventor's Signature Jun Kamada Date May 17, 2002

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

3-00

Full name of third inventor (given name, family name) Takahisa HATAKEYAMA

Inventor's Signature Takahisa Hatakeyama Date May 17, 2002

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

4-00

Full name of fourth inventor (given name, family name) Takayuki HASEBE

Inventor's Signature Takayuki Hasebe Date May 17, 2002

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

5-00

Full name of fifth inventor (given name, family name) Seigou KOTANI

Inventor's Signature Seigou Kotani Date May 17, 2002

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

6-00

Full name of sixth inventor (given name, family name) Shigeki FURUTA

Inventor's Signature Shigeki Furuta Date May 17, 2002

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

Full name of seventh inventor (given name, family name) Takeaki ANAZAWA

Inventor's Signature _____ Date _____

Residence Minato-ku, Tokyo, Japan Citizenship Japanese

Post Office Address c/o NIPPON COLUMBIA CO., LTD., 14-14, Akasaka 4-chome, Minato-ku, Tokyo 107-8011 Japan

Full name of eighth inventor (given name, family name) Toshiaki HIOKI

Inventor's Signature _____ Date _____

Residence Ogaki-shi, Gifu, Japan Citizenship Japanese

Post Office Address c/o SANYO ELECTRIC CO., LTD., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677 Japan

Full name of ninth inventor (given name, family name) Miwa KANAMORI

Inventor's Signature _____ Date _____

Residence Ogaki-shi, Gifu, Japan Citizenship Japanese

Post Office Address c/o SANYO ELECTRIC CO., LTD., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677 Japan

Full name of tenth inventor (given name, family name) Yoshihiro HORI

Inventor's Signature _____ Date _____

Residence Gifu-shi, Gifu, Japan Citizenship Japanese

Post Office Address c/o SANYO ELECTRIC CO., LTD., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677 Japan

Full name of eleventh inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____

Post Office Address

Full name of twelfth inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____

Post Office Address

Full name of thirteenth inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____

Post Office Address

Docket No. P806-698-A020234

Armstrong, Westerman & Hattori, LLP

DECLARATION FOR U.S. PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention **entitled**

Data Reproduction Apparatus and Data Reproduction Module

the specification of which is attached hereto unless the following is checked

☒ was filed on August 29, 2000 as PCT International Application Number PCT/JP00/05832 and was amended on June 20, 2001 (if applicable).

☒ was filed on February 28, 2002 as United States Application Number 10/069,118 and was amended on February 28, 2002 (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 (a) - (d) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application for which priority is claimed.

	(Number)	(Country)	(Day/Month/Year Filed)	Priority Claimed
(List prior foreign applications. See note A)	11-243583 Pat.	Japan	30/August/1999	x Yes __ No
	11-343707 Pat.	Japan	02/December/1999	x Yes __ No
				__ Yes __ No
				__ Yes __ No

(See note B) __ See attached list for additional prior foreign applications

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

	(Application Serial No.)	(Filing Date)	Status
(List prior U.S. Applications)			__ Patented __ Pending __ Abandoned
			__ Patented __ Pending __ Abandoned
			__ Patented __ Pending __ Abandoned
			__ Patented __ Pending __ Abandoned

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

23850

PATENT TRADEMARK OFFICE

Please direct all communications to the following address:

23850

PATENT TRADEMARK OFFICE

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18 of the United States Code, § 1001 and that such willful false statements my jeopardize the validity of the application or any patent issued thereon.

(See note C) Full name of sole or first inventor (given name, family name) Masayuki HATANAKA

Inventor's Signature _____ Date _____

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

Full name of second inventor (given name, family name) Jun KAMADA

Inventor's Signature _____ Date _____

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

Full name of third inventor (given name, family name) Takahisa HATAKEYAMA

Inventor's Signature _____ Date _____

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

Full name of fourth inventor (given name, family name) Takayuki HASEBE

Inventor's Signature _____ Date _____

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

Full name of fifth inventor (given name, family name) Seigou KOTANI

Inventor's Signature _____ Date _____

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

Full name of sixth inventor (given name, family name) Shigeki FURUTA

Inventor's Signature _____ Date _____

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

7-00

Full name of seventh inventor (given name, family name) Takeaki ANAZAWA
Inventor's Signature _____ Date May 7, 2002
Residence Minato-ku, Tokyo, Japan Citizenship Japanese
Post Office Address c/o NIPPON COLUMBIA CO., LTD., 14-14, Akasaka 4-chome, Minato-ku, Tokyo 107-8011 Japan

Full name of eighth inventor (given name, family name) Toshiaki HIOKI
Inventor's Signature _____ Date _____
Residence Ogaki-shi, Gifu, Japan Citizenship Japanese
Post Office Address c/o SANYO ELECTRIC CO., LTD., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677 Japan

Full name of ninth inventor (given name, family name) Miwa KANAMORI
Inventor's Signature _____ Date _____
Residence Ogaki-shi, Gifu, Japan Citizenship Japanese
Post Office Address c/o SANYO ELECTRIC CO., LTD., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677 Japan

Full name of tenth inventor (given name, family name) Yoshihiro HORI
Inventor's Signature _____ Date _____
Residence Gifu-shi, Gifu, Japan Citizenship Japanese
Post Office Address c/o SANYO ELECTRIC CO., LTD., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677 Japan

Full name of eleventh inventor (given name, family name) _____
Inventor's Signature _____ Date _____
Residence _____ Citizenship _____
Post Office Address

Full name of twelfth inventor (given name, family name) _____
Inventor's Signature _____ Date _____
Residence _____ Citizenship _____
Post Office Address

Full name of thirteenth inventor (given name, family name) _____
Inventor's Signature _____ Date _____
Residence _____ Citizenship _____
Post Office Address

Docket No. P806-698-A020234

Armstrong, Westerman & Hattori, LLP

DECLARATION FOR U.S. PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention **entitled**

Data Reproduction Apparatus and Data Reproduction Module

the specification of which is attached hereto unless the following is checked

☒ was filed on August 29, 2000 as PCT International Application Number PCT/JP00/05832 and was amended on June 20, 2001 (if applicable).

☒ was filed on February 28, 2002 as United States Application Number 10/069,118 and was amended on February 28, 2002 (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 (a) - (d) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application for which priority is claimed.

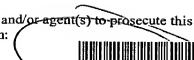
				Priority Claimed
(List prior foreign applications. See note A)	11-243583 Pat. (Number)	Japan (Country)	30/August/1999 (Day/Month/Year Filed)	x Yes ___ No
	11-343707 Pat. (Number)	Japan (Country)	02/December/1999 (Day/Month/Year Filed)	x Yes ___ No
	___ (Number)	___ (Country)	___ (Day/Month/Year Filed)	___ Yes ___ No
	___ (Number)	___ (Country)	___ (Day/Month/Year Filed)	___ Yes ___ No

(See note B) ___ See attached list for additional prior foreign applications

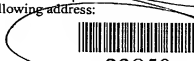
I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

			Status
(List prior U.S. Applications)	___ (Application Serial No.)	___ (Filing Date)	___ Patented ___ Pending ___ Abandoned
	___ (Application Serial No.)	___ (Filing Date)	___ Patented ___ Pending ___ Abandoned
	___ (Application Serial No.)	___ (Filing Date)	___ Patented ___ Pending ___ Abandoned
	___ (Application Serial No.)	___ (Filing Date)	___ Patented ___ Pending ___ Abandoned

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:



Please direct all communications to the following address:



I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18 of the United States Code, § 1001 and that such willful false statements my jeopardize the validity of the application or any patent issued thereon.

1.00

(See note C) Full name of sole or first inventor (given name, family name) Masayuki HATANAKA

Inventor's Signature _____ Date _____

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

2.00

Full name of second inventor (given name, family name) Jun KAMADA

Inventor's Signature _____ Date _____

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

3.00

Full name of third inventor (given name, family name) Takahisa HATAKEYAMA

Inventor's Signature _____ Date _____

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

4.00

Full name of fourth inventor (given name, family name) Takayuki HASEBE

Inventor's Signature _____ Date _____

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

5.00

Full name of fifth inventor (given name, family name) Seigou KOTANI

Inventor's Signature _____ Date _____

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

6.00

Full name of sixth inventor (given name, family name) Shigeki FURUTA

Inventor's Signature _____ Date _____

Residence Kawasaki-shi, Kanagawa, Japan Citizenship Japanese

Post Office Address c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

Full name of seventh inventor (given name, family name) Takeaki ANAZAWA
Inventor's Signature _____ Date _____
Residence Minato-ku, Tokyo, Japan Citizenship Japanese
Post Office Address c/o NIPPON COLUMBIA CO., LTD., 14-14, Akasaka 4-chome, Minato-ku, Tokyo 107-8011 Japan

8-00

Full name of eighth inventor (given name, family name) Toshiaki HIOKI
Inventor's Signature Toshiaki Hioki Date Apr. 26, 2002
Residence Ogaki-shi, Gifu, Japan JPX Citizenship Japanese
Post Office Address c/o SANYO ELECTRIC CO., LTD., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677 Japan

9-00

Full name of ninth inventor (given name, family name) Miwa KANAMORI
Inventor's Signature Miwa Kanamori Date Apr. 26 2002.
Residence Ogaki-shi, Gifu, Japan JPX Citizenship Japanese
Post Office Address c/o SANYO ELECTRIC CO., LTD., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677 Japan

10-00

Full name of tenth inventor (given name, family name) Yoshihiro HORI
Inventor's Signature Yoshihiro Hori Date Apr. 26. 2002
Residence Gifu-shi, Gifu, Japan JPX Citizenship Japanese
Post Office Address c/o SANYO ELECTRIC CO., LTD., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677 Japan

Full name of eleventh inventor (given name, family name) _____
Inventor's Signature _____ Date _____
Residence _____ Citizenship _____
Post Office Address

Full name of twelfth inventor (given name, family name) _____
Inventor's Signature _____ Date _____
Residence _____ Citizenship _____
Post Office Address

Full name of thirteenth inventor (given name, family name) _____
Inventor's Signature _____ Date _____
Residence _____ Citizenship _____
Post Office Address